1. Basic Elements of Statistical Decision Theory and Statistical Learning Theory
2. Elements of Statistical Learning Theory
3. Introduction to Classification and Regression
4. Introduction to Complexity Regularization
5. An Example of the Use of Sieves for Complexity Regularization in Denoising
6. Plug-In Classifier and Histogram Classifier
7. Probably Approximately Correct (PAC) Learning
8. Chernoff's Bound and Hoeffding's Inequality
9. Classification Error Bounds
10. Error Bounds in Countably Infinite Spaces
11. Complexity Regularization
12. Decision Trees
13. Complexity Regularization for Squared Error Loss
14. Maximum Likelihood Estimation
15. Maximum Likelihood and Complexity Regularization
16. Denoising II: Adapting to Unknown Smoothness
17. Nonlinear Approximation and Wavelet Analysis
18. Vapnik-Chervonenkis Theory
19. The Vapnik-Chervonenkis Inequality
20. Applications of VC Bound
21. Lower Performance Bounds for Estimators

Basic Elements of Statistical Decision Theory and Statistical Learning Theory
This paper reviews and contrasts the basic elements of statistical decision theory and statistical learning theory. It is not intended to be a comprehensive treatment of either subject, but rather just enough to draw comparisons between the two.

Throughout this module, let X denote the **input** to a decision-making process and Y denote the correct response or **output** (e.g., the value of a parameter, the label of a class, the signal of interest). We assume that X and Y are random variables or random vectors with joint distribution $P_{X,Y}(x, y)$, where x and y denote specific values that may be taken by the random variables X and Y, respectively. The observation X is used to make decisions pertaining to the quantity of interest. For the purposes of illustration, we will focus on the task of determining the value of the quantity of interest. A decision rule for this task is a function f that takes the observation X as input and outputs a prediction of the quantity Y. We denote a decision rule by $\widehat{Y}$ or $f(X)$, when we wish to indicate explicitly the dependence of the decision rule on the observation. We will examine techniques for designing decision rules and for analyzing their performance.

Measuring Decision Accuracy: Loss and Risk Functions

The accuracy of a decision is measured with a loss function. For example, if our goal is to determine the value of Y, then a loss function takes as inputs the true value Y and the predicted value (the decision) $\widehat{Y} = f(X)$ and outputs a non-negative real number (the "loss") reflective of the accuracy of the decision. Two of the most commonly encountered loss functions include:

1. 0/1 loss: $\ell_{0/1}\left(\widehat{Y}, Y\right) = \mathbf{I}_{\widehat{Y} \neq Y}$, which is the indicator function taking the value of 1 when $\widehat{Y} \neq Y$ and taking the value 0 when $\widehat{Y}(X) = Y$.
2. squared error loss: $\ell_2\left(\widehat{Y}, Y\right) = \| \widehat{Y} - Y \|_2^2$, which is simply the sum of squared differences between the elements of $\widehat{Y}$ and Y.

The 0/1 loss is commonly used in detection and classification problems, and the squared error loss is more appropriate for problems involving the estimation of a continuous parameter. Note that since the inputs to the loss function may be random variables, so is the loss.

A risk $R(f)$ is a function of the decision rule f, and is defined to be the expectation of a loss with respect to the joint distribution $P_{X,Y}(x, y)$. For example, the expected 0/1 loss produces the **probability of error** risk function; i.e., a simply calculation shows

that $R_{0/1}(f) = E[\left(\mathbf{I}_{f(X) \neq Y}\right] = \Pr(f(X) \neq Y)$. The expected squared error loss produces the **mean squared error** MSE risk function, $R_2(f) = E[\| f(X) - Y \|_2^2]$.

Optimal decisions are obtained by choosing a decision rule f that minimizes the desired risk function. Given complete knowledge of the probability distributions involved (e.g., $P_{X,Y}(x, y)$) one can explicitly or numerically design an optimal decision rule, denoted f^*, that minimizes the risk function.

The Maximum Likelihood Principle

The conditional distribution of the observation X given the quantity of interest Y is denoted by $P_{X|Y}(x|y)$. The conditional distribution $P_{X|Y}(x|y)$ can be viewed as a generative model, probabilistically describing the observations resulting from a given value, y, of the quantity of interest. For example, if y is the value of a parameter, the $P_{X|Y}(x|y)$ is the probability distribution of the observation X when the parameter value is set to y. If X is a continuous random variable with conditional density $p_{X|Y}(x|y)$ or a discrete random variable with conditional probability mass function (pmf) $p_{X|Y}(x|y)$, then given a value y we can assess the probability of a particular measurment value y by the magnitude of either the conditional density or pmf.

In decision making problems, we know the value of the observation, but do not know the value y. Therefore, it is appealing to consider the conditional density or pmf as a function of the unknown values y, with X fixed at its observed value. The resulting function is called the likelihood function. As the name suggests, values of y where the likelihood function is largest are intuitively reasonable indicators of the true value of the unknown quantity, which we will denote by y^*. The rationale for this is that these values would produce conditional densities or pmfs that place high probability on the observation $X = x$.

The Maximum Likelihood Estimator (MLE) is defined to be the value of y that maximizes the likelihood function; i.e., in the continuous case
Equation:

$$\hat{y}(X) = \operatorname*{argmax}_y p_{X|Y}(X|y)$$

with an analogous definition for the discrete case by replacing the conditional density with the conditional pmf. The decision rule $\hat{y}(X)$ is called an “estimator,” which is common in decision problems involving a continuous parameter. Note that maximizing the likelihood function is equivalent to minimizing the negative log-likelihood function

(since the logarithm is a monotonic transformation). Now let y^* denote the true value of Y. Then we can view the negative log-likelihood as a loss function
Equation:

$$\ell_L\left(y, y^*\right) \;=\; -\log p_{X|Y}\left(X|y\right)$$

where the dependence on y^* on the right hand side is embodied in the observation X on the left. An interesting special case of the MLE results when the conditional density $P_{X|Y}\left(X|y\right)$ is a Gaussian, in which case the negative log-likelihood corresponds to a squared error loss function.

Now let us consider the expectation of this loss, with respect to the conditional distribution $P_{X|Y}\left(X\middle|y^*\right)$:
Equation:

$$-E\left[\log p_{X|Y}\left(X|y\right)\right] \;=\; \int \log\left(\frac{1}{p_{X|Y}\left(x|y\right)}\right) p_{X|Y}\left(x\middle|y^*\right) dx$$

The true value y^* minimizes the expected negative log-likelihood (or, equivalently, maximizes the expected log-likelihood). To see this, compare the expected log-likelihood of y^* with that of any other value y:
Equation:

$$\begin{aligned} E\left[\log p_{X|Y}\left(X\middle|y^*\right) - \log p_{X|Y}\left(X|y\right)\right] &= E\left[\log\left(\frac{p_{X|Y}\left(X\middle|y^*\right)}{p_{X|Y}\left(X|y\right)}\right)\right] \\ &= \int \log\left(\frac{p_{X|Y}\left(x\middle|y^*\right)}{p_{X|Y}\left(x|y\right)}\right) p_{X|Y}\left(x\middle|y^*\right) dx. \\ &= \mathrm{KL}\left(p_{X|Y}\left(x\middle|y^*\right), p_{X|Y}\left(x|y\right)\right) \end{aligned}$$

The quantity $\mathrm{KL}\left(p_{X|Y}\left(x\middle|y^*\right), p_{X|Y}\left(x|y\right)\right)$ is called the Kullback-Leibler (KL) divergence between the conditional density function $p_{X|Y}\left(x\middle|y^*\right)$ and $p_{X|Y}\left(x|y\right)$. The KL divergence is non-negative, and zero if and only if the two densities are equal [link]. So, we see that the KL divergence acts as a sort of risk function in the context of Maximum Likelihood Estimation.

The Cramer-Rao Lower Bound

The MLE is based on finding the value for Y that maximizes the likelihood function. Intuitively, if the maximum point is very distinct, say a well isolated peak in the likelihood function, then the easier it will be to distinguish the MLE from alternative decisions. Consider the case in which Y is a scalar quantity. The "peakiness" of the log-likelihood function can be gauged by examining its curvature, $-\frac{\partial^2 \log p_{X|Y}(x|y)}{\partial y^2}$, at the point of maximum likelihood. The higher the curvature, the more peaky is the behavior of the likelihood function at the maximum point. Of course, we hope that the MLE will be a good predictor (decision) for the unknown true value y^*. So, rather than looking at the curvature of the log-likelihood function at the maximum likelihood point, a more appropriate measure of how easily it will be to distinguish y^* from the alternatives is the expected curvature of the log-likelihood function evaluated at the value y^*. The expectation taken over all possible observations with respect to the conditional density $p_{X|Y}\left(x\middle|y^*\right)$. This quantity, denoted $I\left(y^*\right) = E\left[-\frac{\partial^2 \log p_{X|Y}(x|y)}{\partial y^2}\right]\Big|_{y=y^*}$, is called the Fisher Information (FI). In fact, the FI provides us with an important performance bound known as the Cramer-Rao Lower Bound (CRLB).

The CRLB states that under some mild regularity assumptions about the conditional density function $p_{X|Y}\left(x|y\right)$, the variance of any unbiased estimator is bounded from below by the inverse of the $I\left(y^*\right)$[link], [link], [link]. Recall that an unbiased estimator is any estimator $\widehat{Y}$ that satisfies $E\left[\widehat{Y}\right] = y^*$. The CRLB tells us is that

Equation:

$$\text{var}\left(\widehat{Y}\right) \;\geq\; \frac{1}{I\left(y^*\right)}.$$

If Y is a vector-valued quantity, then the expected negative Hessian matrix (matrix of partial second derivatives) of the log-likelihood function is called the Fisher Information Matrix (FIM), and a similar inequality tells us that the variance of each component of any unbiased estimator of y^* is bounded below by the corresponding diagonal element of the inverse of the FIM. Since the MSE of an unbiased estimator is equal to its variance, we see that the CRLB provides a very useful lower bound on the best MSE performance that we can hope to achieve. Thus, the CRLB is often used as a comparison point for evaluating estimators. It may or may not be possible to achieve the CRLB, but if we find a decision rule that does, we know that it also minimizes the MSE risk among all possible unbiased estimators. In general, it may be difficult to compute the CRLB, but in certain important cases it is possible to find closed-form or computational solutions.

Bayesian Decision Theory

Bayesian Decision Theory provides a formal system for integrating prior knowledge and observed observations. For the purposes of illustration we will focus on problems involving continuous variables and observations, but extensions to discrete cases are straightforward (simple replace probability densities with probability mass functions, and integrals with summations). The key elements of Bayesian methods are:

1. a prior probability density function $p_Y(y)$ describing a priori knowledge of probable states for the quantity Y;
2. the likelihood function $p_{X|Y}(x|y)$, as described above;
3. the posterior density function $p_{Y|X}(y|x)$.

The posterior density is a function of the prior and likelihood, obtained according to Bayes rule:
Equation:

$$p_{Y|X}(y|x) = \frac{p_{X|Y}(x|y)p_Y(y)}{\int p_{X|Y}(x|y)p_Y(y)dy}.$$

The posterior is an indicator of probable values for Y, based on the prior knowledge and the observation. Several options exist for deriving a specific estimate of Y using the posterior. The mean value of the posterior density is one common choice (commonly called the **posterior mean**). The posterior mean is the decision rule that minimizes the expected squared error loss (MSE risk) function. The value y where the posterior density is maximized is another popular estimator (commonly called the **Maximum A Posteriori** (MAP) estimator). Note that the denominator of the posterior is independent of y, so the MAP estimator is simply the maximizer of the product of the likelihood and the prior. Therefore, if the prior is a constant function, the MAP estimator and MLE coincide.

Statistical Learning

In all of the methods described above, we assumed some amount of knowledge about the distributions of the observation X and quantity of interest Y. Such knowledge can come from a careful analysis of the physical characteristics of the problem at hand, or it can be gleaned from previous experience. However, there are situations where it is difficult to model the physics of the problem and we may not have enough experience to develop complete and accurate probability models. In such cases, it is natural to adopt a **statistical learning** approach [link], [link].

Statistical learning methods are based on developing decision rules or estimators based only on a collection of training examples, rather than predetermined probability models.

Statistical learning methods are often said to be **distribution-free**, since they do not assume particular probability models. The canonical set-up for statistical learning is as follows. We begin with a collection of training examples, $\{(X_i, Y_i)\}_{i=1}^n$, which are assumed to be independently and identically distributed according to an **unknown** probability distribution $P_{X,Y}(x, y)$. If we knew $P_{X,Y}(x, y)$, then we could compute a desired risk function and design an optimal decision rule using the methods described above. In essence, the training examples give us a glimpse at the underlying distribution, but our knowledge of it is far from complete. We cannot exactly compute a risk function, and therefore we cannot derive a corresponding optimal decision rule.

There are at least two ways to proceed at this point. One possibility is to use the training examples to estimate the joint probability distribution, and then use this estimate to derive an decision rule. Unfortunately, the (general-purpose) problem of estimating a distribution is often more difficult from a limited pool of data than is the problem of designing a specific-purpose decision rule. For this reason, a second possibility is more commonly favored in practice. Rather than estimating the complete distribution, one can use the training examples to directly design a decision rule. More precisely, perhaps the most common approach is to use the training examples to compute an estimate of the desired risk function.

Suppose that we are interested in minimizing a particular risk function. Recall that the risk is the expected value of a chosen loss function. Let $\ell\left(\widehat{Y}, Y\right)$ denote the loss, and let $f(X)$ denote a candidate decision function, mapping observations to predictions about Y (i.e., $\widehat{Y} = f(X)$). The **empirical risk function** is constructed from the training examples as follows:
Equation:

$$\widehat{R}(f) \;=\; \frac{1}{n}\sum_{i=1}^{n} \ell\left(f\left(X_i\right), Y_i\right).$$

This is simply the average loss of the decision rule f over the set of training examples. Note that since the training examples are independent and identically distributed, the expected value of the empirical risk is equal to the true risk $R(f) = E[\ell(f(X), Y)]$. Moreover, we known (according to the law of large numbers) that the empirical risk tends to the true risk as the size of the training sample increases. These facts lend support to the idea of choosing a decision rule to minimize the empirical risk.

Empirical risk minimization (ERM) is just this process. Given a collection of possible decision rules, say $\mathscr{F}$, ERM selects a decision rule according to
Equation:

$$\widehat{f}_n \;=\; \operatorname*{argmin}_{f \in \mathscr{F}} \widehat{R}\,(f).$$

The selected rule, $\widehat{f}_n$, obviously depends on the given set of training examples, and therefore it is itself a random quantity. The theoretically optimal counterpart to $\widehat{f}_n$ is the decision rule that minimizes the true risk
Equation:

$$f^* \;=\; \operatorname*{argmin}_{f \in \mathscr{F}} R\,(f).$$

The central problem in statistical learning is to quantify how close $\widehat{f}_n$ performs relative to f^*. Note that $R\left(f^*\right) \leq R\left(\widehat{f}_n\right)$, since f^* minimizes the true risk. Thus, one way to gauge the performance of $\widehat{f}_n$ relative to f^* is to show that there exists small positive values ϵ and δ such that with probability at least $1-\delta$ we have
Equation:

$$R\left(\widehat{f}_n\right) \;\leq\; R\left(f^*\right) + \epsilon.$$

If an inequality of this form holds, then we say that $\widehat{f}_n$ is a **Probability Approximately Correct** (PAC) decision rule [link].

To show that the empirical risk minimizer is a PAC decision rule, we first must understand how closely the empirical risk matches the true risk. First, let us consider the empirical and true risk of the decision rule f. Assume that the loss function is bounded between 0 and 1 (possibly after a suitable normalization). Then the empirical risk function is a sum of independent random variables bounded between 0 and 1. Hoeffding's inequality is a bound on the deviations of such random sums from their corresponding mean values [link]. In this case, the mean value is the true risk of f, and Hoeffding's inequality states that
Equation:

$$P(|\widehat{R}\,(f) - R\,(f)\,| > \epsilon) \;\leq\; 2e^{-2n\epsilon^2}.$$

Another equivalent statement is that the inequality $\left|\widehat{R}\,(f) - R\,(f)\right| \leq \epsilon$ holds with probability at least $1 - 2e^{-2n\epsilon^2}$. Thus, the two risks are probably close together, and the greater the number of training examples, n, the closer they are.

Now we would like a similar condition to hold for all $f \in \mathscr{F}$, since ERM optimizes over the entire collection $\mathscr{F}$. Suppose that $\mathscr{F}$ is a finite collection of decision rules. Let $|\mathscr{F}|$ denote the number of rules in $\mathscr{F}$. The probability that the difference between the true and empirical risks, of one or more of the decision rules, exceeds ϵ is bounded by the sum of the probabilities of each individual event of the form $\left|\widehat{R}\left(f\right) - R\left(f\right)| > \epsilon$, the so-called **Union of Events** bound. Therefore, with probability at least $1 - |\mathscr{F}|2e^{-2n\epsilon^2}$ we have that
Equation:

$$\left|\widehat{R}\left(f\right) - R\left(f\right)| \leq \epsilon$$

for all $f \in \mathscr{F}$. Equivalently, setting $\delta = 2|\mathscr{F}|e^{-2n\epsilon^2}$, we have that with probability at least $1 - \delta$ and for all $f \in \mathscr{F}$
Equation:

$$\left|\widehat{R}\left(f\right) - R\left(f\right)| \leq \sqrt{\frac{\log|\mathscr{F}| + \log\left(2/\delta\right)}{2n}}.$$

Notice that the two risks are uniformly close together, and the closeness indicated by the bound increases as n increases and decreases as the number of decision rules in $\mathscr{F}$ increases. In fact, the bound scales with $\log|\mathscr{F}|$, and so it is reasonable to interpret the logarithm of the number of decision rules under consideration as a measure of the **complexity** of the class.

Now using this bound, we can show that $\widehat{f}_n$ is a PAC decision rule as follows. Note that with probability at least $1 - \delta$
Equation:

$$\begin{aligned} R\left(\widehat{f}_n\right) &\leq \widehat{R}\left(\widehat{f}_n\right) + \sqrt{\frac{\log|\mathscr{F}| + \log\left(2/\delta\right)}{2n}} \\ &\leq \widehat{R}\left(f^*\right) + \sqrt{\frac{\log|\mathscr{F}| + \log\left(2/\delta\right)}{2n}} \\ &\leq R\left(f^*\right) + 2\sqrt{\frac{\log|\mathscr{F}| + \log\left(2/\delta\right)}{2n}} \end{aligned}$$

where the first inequality follows since the true and empirical risks are close for all $f \in \mathscr{F}$, and in particular for $\widehat{f}_n$, the second inequality holds since by definition $\widehat{f}_n$

minimizes the empirical risk, and the third inequality holds again since the empirical risk is close to the true risk for all f, in this case for f^* in particular. So, we have shown that $\widehat{f}_n$ is PAC.

PAC bounds of this form can be extended in many directions, for example to infinitely large or uncountable classes of decision rules, but the basic ingredients of the theory are essentially like those demonstrated above. The bottom line is that empirical risk minimization is a reasonable approach, provided one has access to a sufficient number of training examples and the number, or more generally the complexity, of the class of decision rules under consideration is not too great.

Further reading

Excellent treatments of classical decision and estimation theory can be found in a number of textbooks [link], [link], [link], [link]. For references on statistical learning theory, outstanding textbooks are also available [link], [link], [link] for further reading.

Elements of Statistical Learning Theory

Three Elements of Statistical Data Analysis

- **1. Probabilistic Formulation**of learning from data and prediction problems.
- **2. Performance Characterization:**
    - concentration inequalities
    - uniform deviation bounds
    - approximation theory
    - rates of convergence
- **3. Practical Algorithms**that run in polynomial time (e.g., decision trees, wavelet methods, support vector machines).

Learning from Data

To formulate the basic learning from data problem, we must specify several basic elements: data spaces, probability measures, loss functions, and statistical risk.

Data Spaces

Learning from data begins with a specification of two spaces:
Equation:

$$\mathscr{X} \equiv \text{Input Space}$$

Equation:

$$\mathscr{Y} \equiv \text{Output Space.}$$

The input space is also sometimes called the “feature space” or “signal domain.” The output space is also called the “class label space,” “outcome

space," "response space," or "signal range."

Example:
Equation:

$$\mathscr{X} = \mathbf{R}^d \quad d\text{-dimensional Euclidean space of ``feature vectors''}$$

Equation:

$$\mathscr{Y} = \{0, 1\} \quad \text{two classes or ``class labels''}$$

Example:
Equation:

$$\mathscr{X} = \mathbf{R} \quad \text{one-dimensional signal domain (e.g., time-domain)}$$

Equation:

$$\mathscr{Y} = \mathbf{R} \quad \text{real-valued signal}$$

A classic example is estimating a signal f in noise:
Equation:

$$Y = f(X) + W$$

where X is a random sample point on the real line and W is a noise independent of X.

Probability Measure and Expectation

Define a joint probability distribution on $\mathscr{X} \times \mathscr{Y}$ denoted $P_{X,Y}$. Let (X, Y) denote a pair of random variables distributed according to $P_{X,Y}$. We will also have use for marginal and conditional distributions. Let P_X denote the marginal distribution on X, and let $P_{Y|X}$ denote the conditional distribution of Y given X. For any distribution P, let p denote its density function with respect to the corresponding dominating measure; e.g., **Lebesgue measure** for continuous random variables or **counting measure** for discrete random variables.

Define the expectation operator:
Equation:

$$E_{X,Y}\left[f\left(X, Y\right)\right] \equiv \int f\left(x, y\right) dP_{X,Y}\left(x, y\right) = \int f\left(x, y\right) p_{X,Y}\left(x, y\right) dx dy.$$

We will also make use of corresponding marginal and conditional expectations such as E_X and $E_{Y|X}$.

Wherever convenient and obvious based on context, we may drop the subscripts (e.g., E instead of $E_{X,Y}$) for notational ease.

Loss Functions

A loss function is a mapping
Equation:

$$\ell : \mathscr{Y} \times \mathscr{Y} \mapsto \mathbf{R}.$$

Example:
In binary classification problems, $\mathscr{Y} = \{0, 1\}$. The $0/1$ loss function is usually used: $\ell\left(y_1, y_2\right) = 1_{y_1 \neq y_2}$, where 1_A is the indicator function which takes a value of 1 if condition A is true and zero otherwise. We typically

will compare a true label y with a prediction $\hat{y}$, in which case the $0/1$ loss simply counts misclassifications.

Example:
In regression or estimation problems, $\mathscr{Y} = R$. The squared error loss function is often employed: $\ell\left(y_1, y_2\right) = \left(y_1 - y_2\right)2$, the square of the difference between y_1 and y_2. In application, we are interested in a true value y in comparison to an estimate $\hat{y}$.

Statistical Risk

The basic problem in learning is to determine a mapping $f : \mathscr{X} \mapsto \mathscr{Y}$ that takes an input $x \in \mathscr{X}$ and predicts the corresponding output $y \in \mathscr{Y}$. The performance of a given map f is measured by its expected loss or **risk**:
Equation:

$$R\left(f\right) \equiv E_{X,Y}[\ell(f(X), Y)].$$

The risk tells us how well, on average, the predictor f performs with respect to the chosen loss function. A key quantity of interest is the mininum risk value, defined as
Equation:

$$R^{*} = \inf_{f} \; R\left(f\right)$$

where the infinum is taking over all measurable functions.

The Learning Problem

Suppose that (X, Y) are distributed according to $P_{X,Y}$ ($(X, Y) \sim P_{X,Y}$ for short). Our goal is to find a map so that $f(X) \approx Y$ with high probability. Ideally, we would chose f to minimize the risk $R(f) = E[\ell(f(X), Y)]$. However, in order to compute the risk (and hence optimize it) we need to know the joint distribution $P_{X,Y}$. In many problems of practical interest, the joint distribution is unknown, and minimizing the risk is not possible.

Suppose that we have some exemplary samples from the distribution. Specifically, consider n samples $X_i, Y_i{}_{i=1}^{n}$ distributed independently and identically (iid) according to the otherwise unknown $P_{X,Y}$. Let us call these samples **training data**, and denote the collection by $D_n \equiv X_i, Y_i{}_{i=1}^{n}$. Let's also define a collection of candidate mappings $\mathscr{F}$. We will use the training data D_n to pick a mapping $f_n \in \mathscr{F}$ that we hope will be a good predictor. This is sometimes called the **Model Selection** problem. Note that the selected model f_n is a function of the training data:
Equation:

$$f_n(X) = f(X; D_n),$$

which is what the subscript n in f_n refers to. The risk of f_n is given by
Equation:

$$R(f_n) = E_{X,Y}\left[\ell\left(f_n(X), Y\right)\right].$$

Note that since f_n depends on D_n in addition to a new random pair (X, Y), the risk is a random variable (i.e., a function of the training data D_n). Therefore, we are interested in the **expected risk**, computed over random realizations of the training data:
Equation:

$$E_{D_n}\left[R(f_n)\right].$$

We hope that f_n produces a small expected risk.

The notion of expected risk can be interpreted as follows. We would like to define an algorithm (a model selection process) that performs well on average, over any random sample of n training data. The expected risk is a measure of the expected performance of the algorithm with respect to the chosen loss function. That is, we are not gauging the risk of a particular map $f \in \mathscr{F}$, but rather we are measuring the performance of the algorithm that takes any realization of training data and selects an appropriate model in $\mathscr{F}$.

This course is concerned with determining "good" model spaces $\mathscr{F}$ and useful and effective model selection algorithms.

Introduction to Classification and Regression

Pattern Classification

Recall that the goal of classification is to learn a mapping from the feature space, $\mathscr{X}$, to a label space, $\mathscr{Y}$. This mapping, f, is called a **classifier**. For example, we might have
Equation:

$$\begin{aligned} \mathscr{X} &= \mathbf{R}^d \\ \mathscr{Y} &= \{0,1\}. \end{aligned}$$

We can measure the loss of our classifier using $0-1$ loss; **i.e.,**
Equation:

$$\ell\left(\hat{y}, y\right) = \mathbf{1}_{\{\hat{y} \neq y\}} = \begin{cases} 1, & \hat{y} \neq y \\ 0, & \hat{y} = y \end{cases}.$$

Recalling that risk is defined to be the expected value of the loss function, we have
Equation:

$$R\left(f\right) = E_{XY}[\ell(f(X), Y)] = E_{XY}\left[\mathbf{1}_{\{f(X) \neq Y\}}\right] = P_{XY}(f(X) \neq Y).$$

The performance of a given classifier can be evaluated in terms of how close its risk is to the Bayes' risk.

(Bayes' Risk)
The Bayes' risk is the infimum of the risk for all classifiers:
Equation:

$$R^* = \inf_f R\left(f\right).$$

We can prove that the Bayes risk is achieved by the Bayes classifier.

Bayes Classifier
The Bayes classifier is the following mapping:
Equation:

$$f^*\left(x\right) = \begin{cases} 1, & \eta(x) \geq 1/2 \\ 0, & otherwise \end{cases}$$

where
Equation:

$$\eta\left(x\right) \equiv P_{Y|X}\left(Y = 1 | X = x\right).$$

Note that for any x, $f^*\left(x\right)$ is the value of $y \in \{0,1\}$ that maximizes $P_{XY}\left(Y = y | X = x\right)$.

Theorem
Risk of the Bayes Classifier
Equation:

$$R\left(f^*\right) = R^*.$$

Let $g(x)$ be any classifier. We will show that
Equation:

$$P\left(g\left(X\right) \neq Y | X = x\right) \geq P\left(f^{*}\left(x\right) \neq Y \middle| X = x\right).$$

For any g,
Equation:

$$\begin{aligned} P(g(X) \neq Y | X = x) &= 1 - P(Y = g(X) | X = x) \\ &= 1 - [P(Y = 1, g(X) = 1 | X = x) + P(Y = 0, g(X) = 0 | X = x)] \\ &= 1 - \left[E\left[\mathbf{1}_{\{Y=1\}}\mathbf{1}_{\{g(X)=1\}} \middle| X = x\right] + E\left[\mathbf{1}_{\{Y=0\}}\mathbf{1}_{\{g(X)=0\}} \middle| X = x\right]\right] \\ &= 1 - \left[\mathbf{1}_{\{g(x)=1\}}E\left[\mathbf{1}_{\{Y=1\}} \middle| X = x\right] + \mathbf{1}_{\{g(x)=0\}}E\left[\mathbf{1}_{\{Y=0\}} \middle| X = x\right]\right] \\ &= 1 - \left[\mathbf{1}_{\{g(x)=1\}}P(Y = 1 | X = x) + \mathbf{1}_{\{g(x)=0\}}P(Y = 0 | X = x)\right] \\ &= 1 - \left[\mathbf{1}_{\{g(x)=1\}}\eta\left(x\right) + \mathbf{1}_{\{g(x)=0\}}(1 - \eta(x))\right] \end{aligned}.$$

Next consider the difference
Equation:

$$\begin{aligned} P(g(x) \neq Y | X = x) - P\Big(f^{*}\left(x\right) \neq Y | X = x\Big) & \\ &= \eta\left(x\right)\left[\mathbf{1}_{\{f^{*}(x)=1\}} - \mathbf{1}_{\{g(x)=1\}}\right] + (1 - \eta\left(x\right))\left[\mathbf{1}_{\{f^{*}(x)=0\}} - \right. \\ &= \eta\left(x\right)\left[\mathbf{1}_{\{f^{*}(x)=1\}} - \mathbf{1}_{\{g(x)=1\}}\right] - (1 - \eta\left(x\right))\left[\mathbf{1}_{\{f^{*}(x)=1\}} - \right. \\ &= (2\eta(x) - 1)\Big(\mathbf{1}_{\{f^{*}(x)=1\}} - \mathbf{1}_{\{g(x)=1\}}\Big), \end{aligned}$$

where the second equality follows by noting that $\mathbf{1}_{\{g(x)=0\}} = 1 - \mathbf{1}_{\{g(x)=1\}}$. Next recall
Equation:

$$f^{*}\left(x\right) = \begin{cases} 1, & \eta(x) \geq 1/2 \\ 0, & otherwise \end{cases}.$$

For x such that $\eta(x) \geq 1/2$, we have
Equation:

$$\underbrace{(2\eta(x) - 1)}_{\geq 0}\underbrace{\left(\underbrace{\mathbf{1}_{\{f^{*}(x)=1\}}}_{1} - \underbrace{\mathbf{1}_{\{g(x)=1\}}}_{0 or 1}\right)}_{\geq 0}$$

and for x such that $\eta(x) < 1/2$, we have
Equation:

$$\underbrace{(2\eta(x) - 1)}_{< 0}\underbrace{\left(\underbrace{\mathbf{1}_{\{f^{*}(x)=1\}}}_{0} - \underbrace{\mathbf{1}_{\{g(x)=1\}}}_{0 or 1}\right)}_{\leq 0},$$

which implies
Equation:

$$(2\eta(x)-1)\left(\mathbf{1}_{\{f^*(x)=1\}}-\mathbf{1}_{\{g(x)=1\}}\right)\geq 0$$

or
Equation:

$$P\left(g\left(X\right)\neq Y|X=x\right)\geq P\left(f^{*}\left(x\right)\neq Y\Big|X=x\right).$$

Note that while the Bayes classifier achieves the Bayes risk, in practice this classifier is not realizable because we do not know the distribution P_{XY} and so cannot construct $\eta(x)$.

Regression

The goal of regression is to learn a mapping from the input space, $\mathscr{X}$, to the output space, $\mathscr{Y}$. This mapping, f, is called a **estimator**. For example, we might have
Equation:

$$\begin{aligned}\mathscr{X} &= \mathbf{R}^{d}\\ \mathscr{Y} &= \mathbf{R}.\end{aligned}$$

We can measure the loss of our estimator using squared error loss; **i.e.,**
Equation:

$$\ell\left(\hat{y},y\right)=\left(y-\hat{y}\right)^{2}.$$

Recalling that risk is defined to be the expected value of the loss function, we have
Equation:

$$R\left(f\right)=E_{XY}\left[\ell\left(f\left(X\right),Y\right)\right]=E_{XY}\left[\left(f\left(X\right)-Y\right)^{2}\right].$$

The performance of a given estimator can be evaluated in terms of how close the risk is to the infimum of the risk for all estimator under consideration:
Equation:

$$R^{*}=\inf_{f}R\left(f\right).$$

Theorem
Minimum Risk under Squared Error Loss (MSE)

Let $f^{*}\left(x\right)=E_{Y|X}\left[Y|X=x\right]$
Equation:

$$R\left(f^{*}\right)=R^{*}.$$

Equation:

$$
\begin{aligned}
R(f) &= E_{XY}\left[(f(X)-Y)^2\right] \\
&= E_X\left[E_{Y|X}\left[(f(X)-Y)^2|X\right]\right] \\
&= E_X\left[E_{Y|X}\left[\left(f(X)-E_{Y|X}[Y|X]+E_{Y|X}[Y|X]-Y\right)^2|X\right]\right] \\
&= \begin{aligned}[t] E_X[& E_{Y|X}\left[\left(f(X)-E_{Y|X}[Y|X]\right)^2\middle|X\right] \\ & +2E_{Y|X}\left[\left(f(X)-E_{Y|X}[Y|X]\right)\left(E_{Y|X}[Y|X]-Y\right)|X\right] \\ & +E_{Y|X}\left[\left(E_{Y|X}[Y|X]-Y\right)^2\middle|X\right]\Big] \end{aligned} \\
&= \begin{aligned}[t] E_X[& E_{Y|X}\left[\left(f(X)-E_{Y|X}[Y|X]\right)^2\middle|X\right] \\ & +2\left(f(X)-E_{Y|X}[Y|X]\right)\times 0 \\ & +E_{Y|X}\left[\left(E_{Y|X}[Y|X]-Y\right)^2\middle|X\right]\Big] \end{aligned} \\
&= E_{XY}\left[\left(f(X)-E_{Y|X}[Y|X]\right)^2\right]+R\left(f^*\right).
\end{aligned}
$$

Example:
Thus if $f^*(x)=E_{Y|X}[Y|X=x]$, then $R\left(f^*\right)=R^*$, as desired.

Empirical Risk Minimization

Empirical Risk

Let $\{X_i,Y_i\}_{i=1}^n \overset{iid}{\sim} P_{XY}$ be a collection of training data. Then the empirical risk is defined as
Equation:

$$\widehat{R}_n(f)=\frac{1}{n}\sum_{i=1}^n \ell\left(f(X_i),Y_i\right).$$

Empirical risk minimization is the process of choosing a learning rule which minimizes the empirical risk;
i.e.,
Equation:

$$\widehat{f}_n = \operatorname*{argmin}_{f\in\mathscr{F}} \widehat{R}_n(f).$$

Example:
Pattern Classification
Let the set of possible classifiers be
Equation:

$$\mathscr{F} = \left\{ x \mapsto \operatorname{sign}\left(w'x\right) : w \in \mathbf{R}^d \right\}$$

and let the feature space, $\mathscr{X}$, be $[0,1]^d$ or $\mathbf{R}^d$. If we use the notation $f_w(x) \equiv \operatorname{sign}(w'x)$, then the set of classifiers can be alternatively represented as

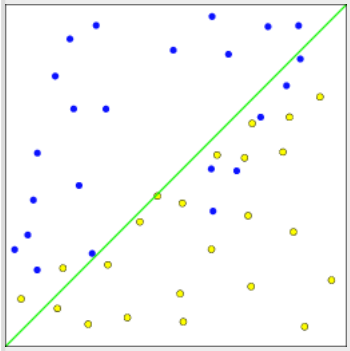
Equation:

$$\mathscr{F} = \left\{ f_w : w \in \mathbf{R}^d \right\}.$$

In this case, the classifier which minimizes the empirical risk is

Equation:

$$\begin{aligned} \widehat{f}_n &= \operatorname*{argmin}_{f \in \mathscr{F}} \widehat{R}_n(f) \\ &= \operatorname*{arg\,min}_{w \in \mathbf{R}^d} \frac{1}{n} \sum_{i=1}^{n} \mathbf{1}_{\{\operatorname{sign}(w'X_i) \neq Y_i\}}. \end{aligned}$$



Example linear classifier for two-class problem.

Example:

Regression

Let the feature space be

Equation:

$$\mathscr{X} = [0,1]$$

and let the set of possible estimators be

Equation:

$$\mathscr{F} = \{\text{degree } d \text{ polynomials on } [0,1]\}.$$

In this case, the classifier which minimizes the empirical risk is

Equation:

$$\begin{aligned} \widehat{f}_n &= \operatorname*{argmin}_{f \in \mathscr{F}} \widehat{R}_n(f) \\ &= \operatorname*{argmin}_{f \in \mathscr{F}} \frac{1}{n} \sum_{i=1}^{n} \left(f(X_i) - Y_i\right)^2. \end{aligned}$$

Alternatively, this can be expressed as
Equation:

$$\begin{aligned} \widehat{w} &= \arg\min_{w \in \mathbf{R}^{d+1}} \frac{1}{n} \sum_{i=1}^{n} \left(w_0 + w_1 X_i + ... + w_d X_i^d - Y_i \right)^2 \\ &= \arg\min_{w \in \mathbf{R}^{d+1}} \| Vw - Y \|^2 \end{aligned}$$

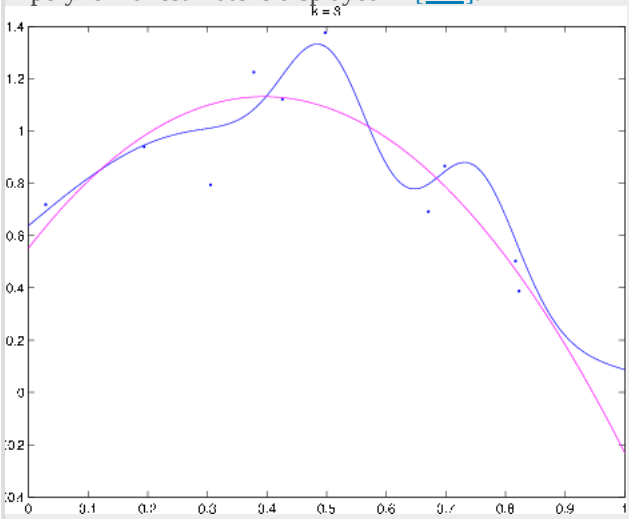
where V is the Vandermonde matrix
Equation:

$$V = \begin{bmatrix} 1 & X_1 & ... & X_1^d \\ 1 & X_2 & ... & X_2^d \\ \vdots & \vdots & \ddots & \vdots \\ 1 & X_n & ... & X_n^d \end{bmatrix}.$$

The pseudoinverse can be used to solve for $\widehat{w}$:
Equation:

$$\widehat{w} = \left(V'V \right)^{-1} V'Y.$$

A polynomial estimate is displayed in [link].



Example polynomial estimator. Blue curve denotes f^*, magenta curve is the polynomial fit to the data (denoted by dots).

Overfitting

Suppose $\mathscr{F}$, our collection of candidate functions, is very large. We can always make
Equation:

$$\min_{f \in \mathscr{F}} \widehat{R}_n(f)$$

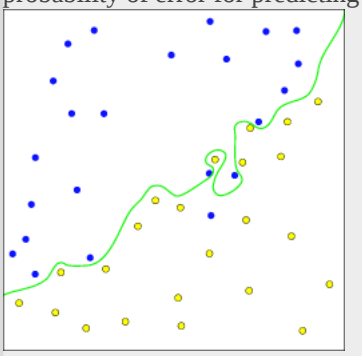
smaller by increasing the cardinality of $\mathscr{F}$, thereby providing more possibilities to fit to the data.

Consider this extreme example: Let $\mathscr{F}$ be all measurable functions. Then every function f for which
Equation:

$$f(x) = \begin{cases} Y_i, & x = X_i \text{ for } i = 1, ..., n \\ \text{any value}, & \text{otherwise} \end{cases}$$

has zero empirical risk ($\widehat{R}_n(f) = 0$). However, clearly this could be a very poor predictor of Y for a new input X
.

Example:
Classification Overfitting
Consider the classifier in [link]; this demonstrates overfitting in classification. If the data were in fact generated from two Gaussian distributions centered in the upper left and lower right quadrants of the feature space domain, then the optimal estimator would be the linear estimator in [link]; the overfitting would result in a higher probability of error for predicting classes of future observations.



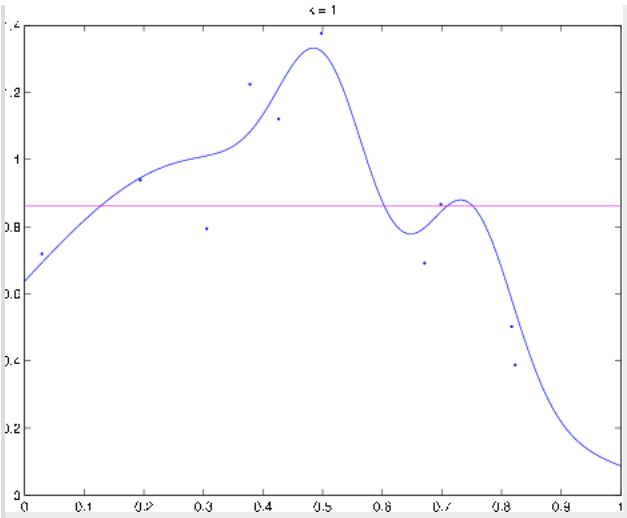
Example of overfitting classifier. The classifier's decision boundary wiggles around in order to correctly label the training data, but the optimal Bayes classifier is a straight line.

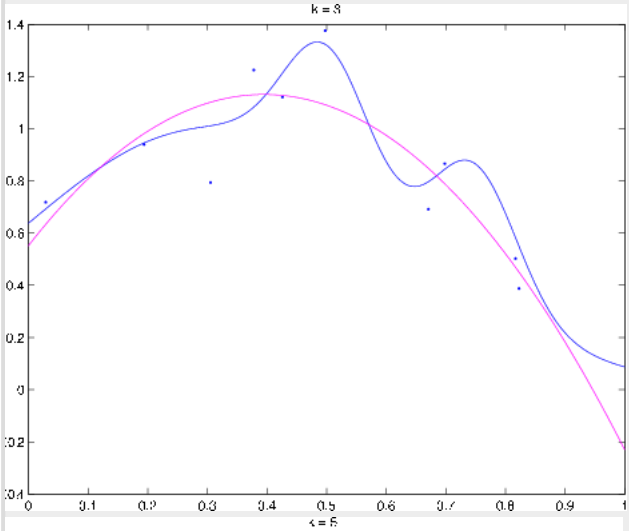
Example:
Regression Overfitting
Below is an m-file that simulates the polynomial fitting. Feel free to play around with it to get an idea of the overfitting problem.

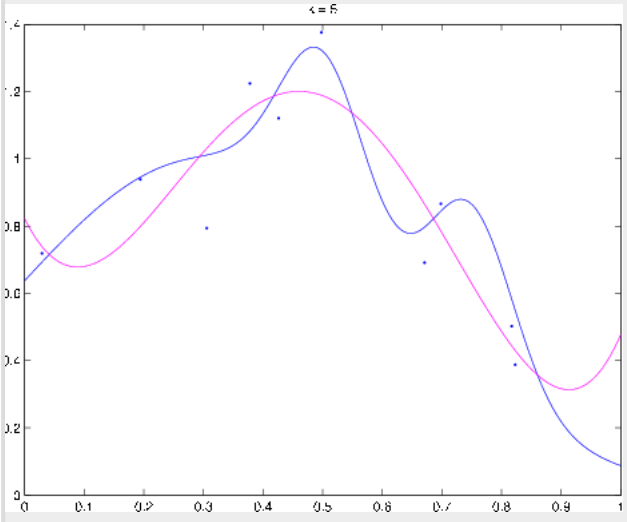
```
% poly fitting
% rob nowak  1/24/04
```

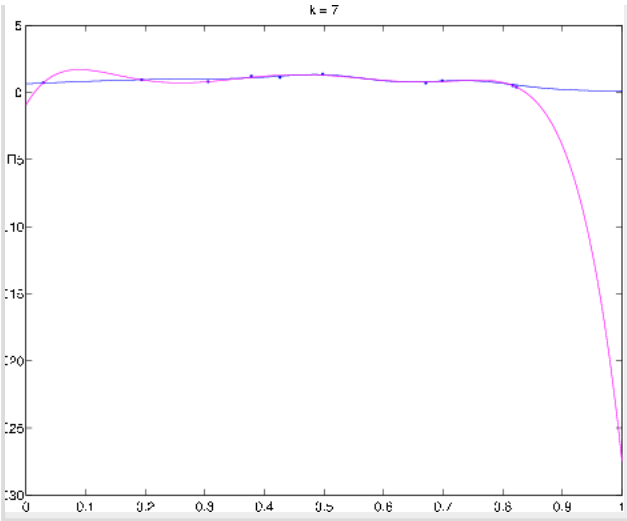
```
clear
close all

% generate and plot "true" function
t = (0:.001:1)';
f = exp(-5*(t-.3).^2)+.5*exp(-100*(t-.5).^2)+.5*exp(-100*(t-.75).^2);
figure(1)
plot(t,f)

% generate n training data & plot
n = 10;
sig = 0.1; % std of noise
x = .97*rand(n,1)+.01;
y = exp(-5*(x-.3).^2)+.5*exp(-100*(x-.5).^2)+.5*exp(-100*
(x-.75).^2)+sig*randn(size(x));
figure(1)
clf
plot(t,f)
hold on
plot(x,y,'.')

% fit with polynomial of order k  (poly degree up to k-1)
k=3;
for i=1:k
    V(:,i) = x.^(i-1);
end
p = inv(V'*V)*V'*y;

for i=1:k
    Vt(:,i) = t.^(i-1);
end
yh = Vt*p;
figure(1)
clf
plot(t,f)
hold on
plot(x,y,'.')
plot(t,yh,'m')
```

Example polynomial fitting problem. Blue curve is f^*, magenta curve is the polynomial fit to the data (dots). (a) Fitting a polynomial of degree $d = 0$: This is an example of underfitting (b)$d = 2$ (c) $d = 4$ (d) $d = 6$: This is an example of overfitting. The empirical loss is zero, but clearly the estimator would not do a good job of predicting y when x is close to one.


k = 1


k = 3


k = 5


k = 7
5
0
−5
−10
−15
−20
−25
−30
0
0.1
0.2
0.3
0.4
0.5
0.6
0.7
0.8
0.9
1

Introduction to Complexity Regularization

Competing Goals: The Bias-Variance Tradeoff

We ended the previous lecture with a brief discussion of overfitting. Recall that, given a set of n data points, D_n, and a space of functions (or **models**) $\mathscr{F}$, our goal in solving the learning from data problem is to choose a function $\widehat{f}_n \in \mathscr{F}$ which minimizes the expected risk $E\left[R\left(\widehat{f}_n\right)\right]$, where the expectation is being taken over the distribution P_{XY} on the data points D_n. One approach to avoiding overfitting is to restrict $\mathscr{F}$ to some subset of all measurable function. To gauge the performance of a given f in this case, we examine the difference between the expected risk of f and the Bayes' risk (called the **excess risk**).
Equation:

$$E\left[R\left(\widehat{f}_n\right)\right] - R^* = \underbrace{\left(E\left[R\left(\widehat{f}_n\right)\right] - \inf_{f\in\mathscr{F}} R(f)\right)}_{\text{estimation error}} + \underbrace{\left(\inf_{f\in\mathscr{F}} R(f) - R^*\right)}_{\text{approximation error}}$$

The **approximation error** term quantifies the performance hit incurred by imposing restrictions on $\mathscr{F}$. The **estimation error** term is due to the randomness of the training data, and it expresses how well the chosen function $\widehat{f}_n$ will perform in relation to the best possible f in the class $\mathscr{F}$. This decomposition into stochastic and approximation errors is similar to the bias-variance tradeoff which arises in classical estimation theory. The approximation error is like a bias squared term, and the estimation error is like a variance term. By allowing the space $\mathscr{F}$to be large[footnote] we can make the approximation error as small as we want at the cost of incurring a large estimation error. On the other hand, if $\mathscr{F}$is very small then the approximation error will be large, but the estimation error may be very small. This tradeoff is illustrated in [link].
When we say $\mathscr{F}$is large, we mean that $|\mathscr{F}|$, the number of elements in $\mathscr{F}$, is large.

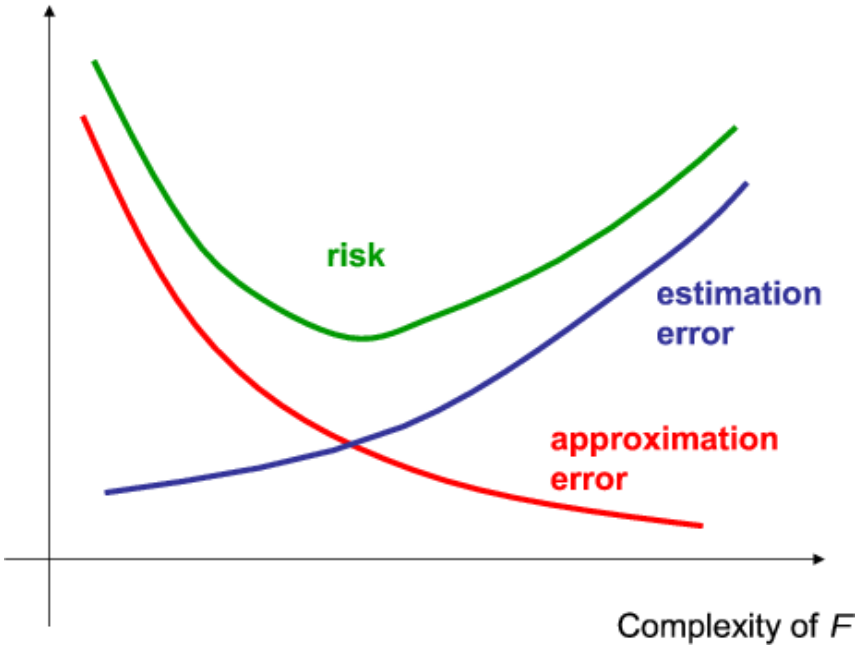


Illustration of tradeoff between estimation and approximation errors as a function of the size (complexity) of the $\mathscr{F}$.

Why is this the case? We do not know the true distribution P_{XY} on the data, so instead of minimizing the expected risk of we design a predictor by minimizing the empirical risk:

Equation:

$$\begin{aligned} \widehat{f}_n &= \operatorname{argmin}_{f \in \mathscr{F}} \widehat{R}_n(f), \\ \widehat{R}_n(f) &= \frac{1}{n} \sum_{i=1}^{n} \ell\left(f\left(X_i\right), Y_i\right). \end{aligned}$$

If $\mathscr{F}$is very large then $\widehat{R}_n(f)$ can be made arbitrarily small and the resulting $\widehat{f}_n$ can "overfit" to the data since $\widehat{R}_n(f)$ is not a good estimator of the true risk $R\left(\widehat{f}_n\right)$.

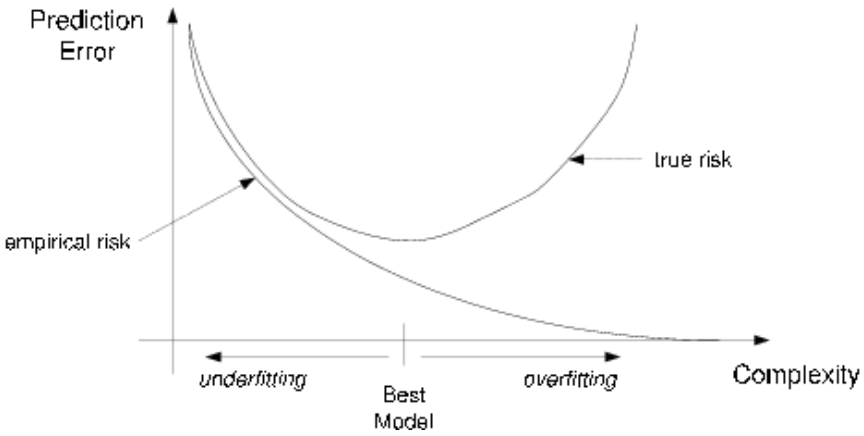


Illustration of empirical risk and the problem of overfitting to the data.

The behavior of the true and empirical risks, as a function of the size (or **complexity**) of the space $\mathscr{F}$, is illustrated in [link]. Unfortunately, we can't easily determine whether we are over or underfitting just by looking at the empirical risk.

Strategies To Avoid Overfitting

Picking
Equation:

$$\widehat{f}_n = \operatorname{argmin}_{f \in \mathscr{F}} \widehat{R}_n(f)$$

is problematic if $\mathscr{F}$ is large. We will examine two general approaches to dealing with this problem:

1. Restrict the size or dimension of $\mathscr{F}$ (e.g., restrict $\mathscr{F}$ to the set of all lines, or polynomials with maximum degree d). This effectively places an upper bound on the estimation error, but in general it also places a lower bound on the approximation error.
2. Modify the empirical risk criterion to include an extra cost associated with each model (e.g., higher cost for more complex models):
   Equation:

$$\widehat{f}_n \;=\; \operatorname*{argmin}_{f\in\mathscr{F}} \Big\{\widehat{R}_n(f) + C(f)\Big\}.$$

The cost is designed to mimic the behavior of the estimation error so that the model selection procedure avoids models with a estimation error. Roughly this can be interpreted as trying to balance the tradeoff illustrated in [link]. Procedures of this type are often called complexity penalization methods.

Example:
Revisit the polynomial regression example (Lecture 2, Ex. 4), and incorporate a penalty term $C(f)$ which is proportional to the degree of f, or the derivative of f. In essence, this approach penalizes for functions which are too "wiggly", with the intuition being that the true function is probably smooth so a function which is very wiggly will overfit the data.
How do we decide how to restrict or penalize the empirical risk minimization process? Approaches which have appeared in the literature include the following.

Method of Sieves

Perhaps the simplest approach is to try to limit the size of $\mathscr{F}$in a way that depends on the number of training data n. The more data we have, the more complex the space of models we can entertain. Let the class of candidate functions grow with n . That is, take
Equation:

$$F_1, \mathscr{F}_2, \cdots, \mathscr{F}_n, \cdots$$

where $|\mathscr{F}_i|$ grows as $i \to \infty$. In other words, consider a sequence of spaces with increasing complexity or degrees of freedom depending on the number of training data samples, n.

Given samples $\{X_i, Y_i\}_{i=1}^n$ i.i.d. distributed according to P_{XY}, select $f \in \mathscr{F}_n$ to minimize the empirical risk
Equation:

$$\widehat{f}_n = \operatorname*{argmin}_{f\in\mathscr{F}_n} \widehat{R}_n(f).$$

In the next lecture we will consider an example using the method of sieves. The basic idea is to design the sequence of model spaces in such a way that the excess risk decays to zero as $n \to \infty$. This sort of idea has been around for decades, but Grenander's method of sieves is often cited as a nice formalization of the idea: **Abstract Inference**, Wiley, New York.

Complexity Penalization Methods

Bayesian Methods

In certain cases, the empirical risk happens to be a (log) likelihood function, and one can then interpret the cost $C(f)$ as reflecting prior knowledge about which models are more or less likely. In this case, $e^{-C(f)}$ is like a prior probability distribution on the space $\mathscr{F}$. The cost $C(f)$ is large if f is highly improbable, and $C(f)$ is small if f is highly probable.

Alternatively, if we restrict $\mathscr{F}$to be small, and denote the space of all measurable functions as $\mathbb{F} = \mathscr{F} \cup \mathscr{F}^c$, then it is essentially as if we have placed a uniform prior over all functions in $\mathscr{F}$, and zero prior probability on the functions in $\mathscr{F}^c$.

Description Length Methods

Description length methods represent each f with a string of bits. More complicated functions require more bits to represent. Accordingly, we can then set the cost $c(f)$ proportional to the number of bits needed to describe f (the **description length**). This results in what is known as the minimum description length (MDL) approach where the minimum description length is given by
Equation:

$$\min_{f \in \mathscr{F}} \left\{ \widehat{R}_n(f) + C(f) \right\}.$$

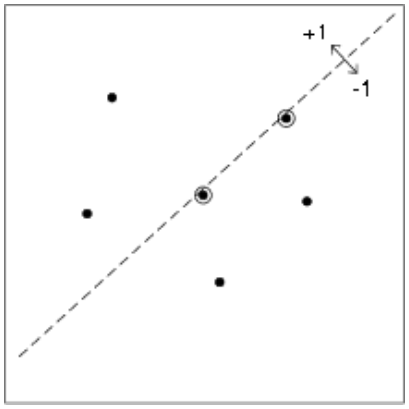
In the Bayesian setting, $p(f) \propto e^{-C(f)}$ can be interpreted as a prior probability density on $\mathscr{F}$, with more complex models being less probable and simpler models

being more probable. In that sense, both the Bayesian and MDL approaches have a similar spirit.

Vapnik-Cervonenkis Dimension

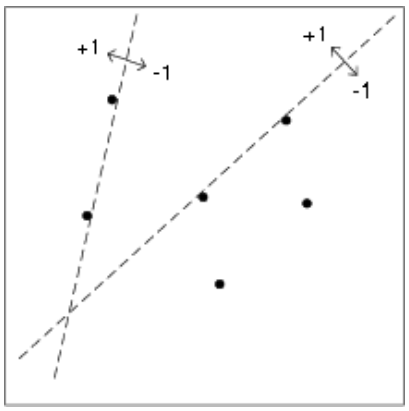
The Vapnik-Cervonenkis (VC) dimension measures the complexity of a class $\mathscr{F}$ relative to a random sample of n training data. For example, take $\mathscr{F}$ to be all linear classifiers in 2-dimensional feature space. Clearly, the space of linear classifiers is infinite (there are an infinite number of lines which can be drawn in the plane). However, many of these linear classifiers would assign the same labels to the training data.

The number of unique labellings of the training data that can be achieved with linear classifiers is, in fact, finite. A line can be defined by picking **any** pair of training points, as illustrated in [link]. Two classifiers can be defined from each such line: one that outputs a label "1" for everything on or above the line, and another that outputs "0" for everything on or above. There exist $\binom{n}{2}$ such pairs of training points, and these define all possible unique labellings of the training data. Therefore, there are at most $2\binom{n}{2}$ unique linear classifiers for any random set of n 2-dimensional features (the factor of 2 is due to the fact that for each linear classifier there are 2 possible assignments of the labelling).



Fitting a linear classifier to 2-dimensional data. There are an infinite number of such

classifiers. We can generate a linear classifier by choosing two data points, drawing a line with both points on one side, and declaring all points on or above the line to be "$+1$" (or "-1") and all points below the line to be "-1" (or "$+1$").



From the discussion in the previous figure, we see that the two linear classifiers depicted in this figure are equivalent for this set of data points, and hence relative to the set of n training data there are only on the order of n^2 unique linear classifiers.

Thus, instead of infinitely many linear classifiers, we realize that as far as a random sample of n training data is concerned, there are at most
Equation:

$$\begin{aligned} 2\binom{n}{2} &= \frac{2n!}{(n-2)!2!} \\ &= n(n-1) \end{aligned}$$

unique linear classifiers. That is, using linear classification rules, there are at most $n\,(n-1) \approx n^2$ unique label assignments for n data points. If we like, we can encode each possibility with $\log_2 n\,(n-1) \approx 2\,\log_2 n$ bits. In d dimensions there are $2\binom{n}{d}$ hyperplane classification rules which can be encoded in roughly $d\,\log_2 n$ bits. Roughly speaking, the number of bits required for encoding each model is the VC dimension. The remarkable aspect of the VC dimension is that it is often finite even when $\mathscr{F}$ is infinite (as in this example).

If $\mathscr{X}$ has d dimensions in total, we might consider linear classifiers based on $1, 2, \cdots, d$ features at a time. Lower dimensional hyperplanes are less complex than higher dimensional ones. Suppose we set
Equation:

$$\begin{aligned} \mathscr{F}_1 &= \text{linear classifiers using 1 feature} \\ \mathscr{F}_2 &= \text{linear classifiers using 2 features.} \\ \cdots & \quad \text{and so on} \end{aligned}$$

These spaces have increasing VC dimensions, and we can try to balance the empirical risk and a cost function depending on the VC dimension. Such procedures are often referred to as **Structural Risk Minimization**. This gives you a glimpse of what the VC dimension is all about. In future lectures we will revisit this topic in greater detail.

Hold-out Methods

The basic idea of "hold-out" methods is to split the n samples $D \equiv \{X_i, Y_i\}_{i=1}^n$ into a training set, D_T, and a test set, D_V.
Equation:

$$D_T = \{X_i, Y_i\}_{i=1}^m, \qquad D_V = \{X_i, Y_i\}_{i=m+1}^n.$$

Now, suppose we have a collection of different model spaces $\{\mathscr{F}_\lambda\}$ indexed by $\lambda \in \Lambda$ (e.g., $\mathscr{F}_\lambda$ is the set of polynomials of degree d, with $\lambda = d$), or suppose that we have a collection of complexity penalization criteria $L_\lambda(f)$ indexed by λ (**e.g.,**let $L_\lambda(f) = \widehat{R}(f) + \lambda c(f)$, with $\lambda \in \mathbf{R}^+$). We can obtain candidate solutions using the training set as follows. Define
Equation:

$$\widehat{R}_m(f) \;=\; \sum_{i=1}^m \ell(f(X_i), Y_i)$$

and take
Equation:

$$\widehat{f}_\lambda \;=\; \operatorname*{argmin}_{f \in \mathscr{F}_\lambda} \widehat{R}_m(f)$$

or
Equation:

$$\widehat{f}_\lambda \;=\; \operatorname*{argmin}_{f \in \mathscr{F}} \left\{ \widehat{R}_m(f) + \lambda c(f) \right\}.$$

This provides us with a set of candidate solutions $\left\{ \widehat{f}_\lambda \right\}$. Then we can define the hold-out error estimate using the test set:
Equation:

$$\widehat{R}_V(f) \;=\; \frac{1}{n-m+1} \sum_{i=m+1}^n \ell(f(X_i), Y_i),$$

and select the “best” model to be $\widehat{f} = \widehat{f}_{\widehat{\lambda}}$ where

Equation:

$$\widehat{\lambda} \;=\; \underset{\lambda}{\operatorname{argmin}}\, \widehat{R}_V\left(\widehat{f}_\lambda\right).$$

This type of procedure has many nice theoretical guarantees, provided both the training and test set grow with n.

Leaving-one-out Cross-Validation

A very popular hold-out method is the so call “leaving-one-out cross-validation” studied in depth by Grace Wahba (UW-Madison, Statistics). For each λ we compute

Equation:

$$\widehat{f}_\lambda^{(k)} \;=\; \underset{f \in \mathscr{F}}{\operatorname{argmin}}\, \frac{1}{n} \sum_{\substack{i=1 \\ i \neq k}}^{n} \ell\left(f\left(X_i\right), Y_i\right) + \lambda C\left(f\right)$$

or

Equation:

$$\widehat{f}_\lambda^{(k)} \;=\; \underset{f \in \mathscr{F}_\lambda}{\operatorname{arg\,min}}\, \frac{1}{n} \sum_{\substack{i=1 \\ i \neq k}}^{n} \ell\left(f\left(X_i\right), Y_i\right).$$

Then we have cross-validation function

Equation:

$$\begin{aligned} V(\lambda) \;&=\; \frac{1}{n} \sum_{k=1}^{n} \ell\left(f_\lambda^{(k)}\left(X_k\right), Y_k\right) \\ \lambda^* \;&=\; \underset{\lambda}{\operatorname{argmin}}\, V\left(\lambda\right). \end{aligned}$$

Summary

To summarize, this lecture gave a brief and incomplete survey of different methods for dealing with the issues of overfitting and model selection. Given a set of training data, $D_n = \{X_i, Y_i\}_{i=1}^n$, our overall goal is to find
Equation:

$$f^* = \operatorname{argmin}_{f \in \mathscr{F}} R(f)$$

from some collection of functions, $\mathscr{F}$. Because we do not know the true distribution P_{XY} underlying the data points D_n, it is difficult to get an exact handle on the risk, $R(f)$. If we only focus on minimizing the empirical risk $\widehat{R}(f)$ we end up overfitting to the training data. Two general approaches were presented.

1. In the first approach we consider an indexed collection of spaces $\{\mathscr{F}_\lambda\}_{\lambda \in \Lambda}$ such that the complexity of $\mathscr{F}_\lambda$ increases as λ increases, and
   Equation:

   $$\lim_{\lambda \to \infty} \mathscr{F}_\lambda = \mathscr{F}.$$

   A solution is given by
   Equation:

   $$\widehat{f}_{\lambda^*} = \arg\min_{f \in \mathscr{F}_{\lambda^*}} \widehat{R}_n(f)$$

   where either λ^* is a function which increases with n,
   Equation:

   $$\lambda^* = \lambda(n),$$

   or λ^* is chosen by hold-out validation.
2. The alternative approach is to incorporate a penalty term into the risk minimization problem formulation. Here we consider an indexed collection of penalties $\{C_\lambda\}_{\lambda \in \Lambda}$ satisfying the following properties:

   1. $C_\lambda : \mathscr{F} \to \mathbf{R}^+$;
   2. For each $f \in \mathscr{F}$ and $\lambda_1 < \lambda_2$ we have $C_{\lambda_1}(f) \leq C_{\lambda_2}(f)$;
   3. There exists $\lambda_0 \in \Lambda$ such that $C_{\lambda_0}(f) = 0$ for all $f \in \mathscr{F}$.

In this formulation we find a solution
Equation:

$$\widehat{f}_{\lambda^*} \quad = \quad \operatorname{argmin}_{f \in \mathscr{F}} \widehat{R}_n(f) + C_{\lambda^*}(f),$$

where either $\lambda^* = \lambda(n)$, a function growing the number of data samples n, or λ^* is selected by hold-out validation.

Consistency

If an estimator or classifier $\widehat{f}_{\lambda^*}$ satisfies
Equation:

$$E\left[R\left(\widehat{f}_{\lambda^*}\right)\right] \to \inf_{f \in \mathscr{F}} R(f) \qquad \text{as } n \to \infty,$$

then we say that $\widehat{f}_{\lambda^*}$ is $\mathscr{F}$-consistent with respect to the risk R. When the context is clear, we will simply say that $\widehat{f}$ is consistent.

An Example of the Use of Sieves for Complexity Regularization in Denoising

Consider the following setting. Let
Equation:

$$Y = f^*(X) + W,$$

where X is a random variable (r.v.) on $\mathscr{X} = [0,1]$, W is a r.v. on $\mathscr{Y} = \mathbf{R}$, independent of X and satisfying
Equation:

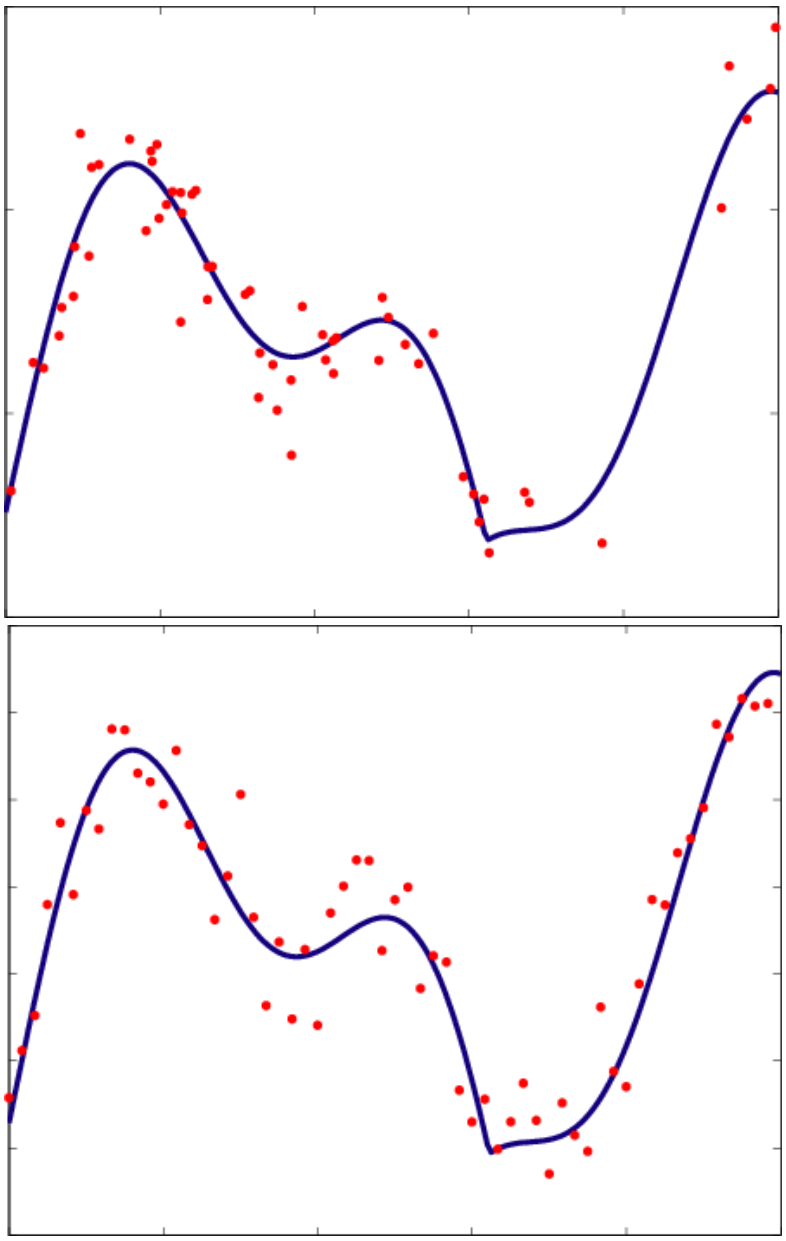
$$E[W] = 0 \quad \text{and} \quad E\left[W^2\right] = \sigma^2 < \infty.$$

Finally let $f^* : [0,1] \to \mathbf{R}$ be a function satisfying
Equation:

$$\left|f^*(t) - f^*(s)\right| \leq L|t-s|, \ \ \forall t, s \in [0,1],$$

where $L > 0$ is a constant. A function satisfying condition [link] is said to be Lipschitz on $[0,1]$. Notice that such a function must be continuous, but it is not necessarily differentiable. An example of such a function is depicted in [link](a).

Example of a Lipschitz function, and our observations setting. (a) random sampling of f^*, the points correspond to $(X_i, Y_i), \ \ i = 1, ..., n$; (b) deterministic sampling of f^*, the points correspond to $(i/n, Y_i), \ \ i = 1, ..., n$.



Note that
Equation:

$$\begin{aligned} E[Y|X=x] &= E\Big[f^*(X)+W\Big|X=x\Big] \\ &= E\Big[f^*(x)+W\Big|X=x\Big] \\ &= f^*(x)+E[W]=f^*(x). \end{aligned}$$

Consider our usual setup: Estimate f^* using n training examples

Equation:

$$\{X_i, Y_i\}_{i=1}^{n} \overset{i.i.d.}{\sim} P_{XY},$$
$$Y_i = f^*(X_i) + W_i,\ \ i = \{1, ..., n\},$$

where $\overset{i.i.d.}{\sim}$ means **independently and identically distributed**. [link](a) illustrates this setup.

In many applications we can sample $\mathscr{X} = [0, 1]$ as we like, and not necessarily at random. For example we can take n samples uniformly on [0,1]
Equation:

$$\begin{aligned} x_i &= \frac{i}{n},\ \ i = 1, ..., n\ , \\ Y_i &= f(x_i) + W_i \\ &= f\left(\frac{i}{n}\right) + W_i. \end{aligned}$$

We will proceed with this setup (as in [link](b)) in the rest of the lecture.

Our goal is to find $\widehat{f}_n$ such that $E\left[\parallel f^* - \widehat{f}_n \parallel^2\right] \to 0,\ \text{as}\ n \to 0$ (here $\parallel \cdot \parallel$ is the usual L_2-norm; i.e., $\parallel f^* - \widehat{f}_n \parallel^2 = \int_0^1 \left|f^*(t) - \widehat{f}_n(t)\right|^2 dt$).

Let
Equation:

$$\mathscr{F} = \{f :\ \ f \text{ is Lipschitz with constant } L\}.$$

The Risk is defined as
Equation:

$$R(f) = \parallel f^* - f \parallel^2 = \int_0^1 \left|f^*(t) - f(t)\right|^2 dt.$$

The Expected Risk (recall that our estimator $\widehat{f}_n$ is based on $\{x_i, Y_i\}$ and hence is a r.v.) is defined as
Equation:

$$E\left[R\left(\widehat{f}_n\right)\right] = E[\| f^* - \widehat{f}_n \|^2].$$

Finally the Empirical Risk is defined as
Equation:

$$\widehat{R}_n(f) = \frac{1}{n}\sum_{i=1}^{n}\left(f\left(\frac{i}{n}\right) - Y_i\right)^2.$$

Let $0 < m_1 \leq m_2 \leq m_3 \leq \cdots$ be a sequence of integers satisfying $m_n \to \infty$ as $n \to \infty$, and $k_n m_n = n$ for some integer $k_n > 0$. That is, for each value of n there is an associated integer value m_n. Define the Sieve $\mathscr{F}_1,\ \mathscr{F}_2,\ \mathscr{F}_3,\ ...,$
Equation:

$$\mathscr{F}_n = \left\{f : f(t) = \sum_{j=1}^{m_n} c_j \mathbf{1}_{\left\{\frac{j-1}{m_n} \leq t < \frac{j}{m_n}\right\}},\ c_j \in \mathbf{R}\right\}.$$

$\mathscr{F}_n$ is the space of functions that are constant on intervals
Equation:

$$\mathrm{I}_{j,m_n} \equiv \left[\frac{j-1}{m_n}, \frac{j}{m_n}\right),\ j = 1, ..., m_n.$$

From here on we will use m and k instead of m_n and k_n (dropping the subscript n) for notational ease. Define
Equation:

$$f_n(t) = \sum_{j=1}^{m} c_j^* \mathbf{1}_{\{t \in I_{j,m}\}}, \quad \text{where} \quad c_j^* = \frac{1}{k}\sum_{i:\frac{i}{n} \in I_{j,m}} f^*\left(\frac{i}{n}\right).$$

Note that $f_n \in \mathscr{F}_n$.

Example:
Exercise 1
Upper bound $\| f^* - f_n \|^2$.
Equation:

$$
\begin{aligned}
\| f^* - f \|^2 &= \int_0^1 \left| f^*(t) - f_n(t) \right|^2 dt \\
&= \sum_{j=1}^{m} \int_{I_{j,m}} \left| f^*(t) - f_n(t) \right|^2 dt \\
&= \sum_{j=1}^{m} \int_{I_{j,m}} \left| f^*(t) - c_j^* \right|^2 dt \\
&= \sum_{j=1}^{m} \int_{I_{j,m}} \left| f^*(t) - \frac{1}{k} \sum_{i:\frac{i}{n} \in I_{j,m}} f^*\left(\frac{i}{n}\right) \right|^2 dt \\
&= \sum_{j=1}^{m} \int_{I_{j,m}} \left(\frac{1}{k} \left| \sum_{i:\frac{i}{n} \in I_{j,m}} \left(f^*(t) - f^*\left(\frac{i}{n}\right) \right) \right| \right)^2 dt \\
&\leq \sum_{j=1}^{m} \int_{I_{j,m}} \left(\frac{1}{k} \sum_{i:\frac{i}{n} \in I_{j,m}} \left| f^*(t) - f^*\left(\frac{i}{n}\right) \right| \right)^2 dt \\
&\leq \sum_{j=1}^{m} \int_{I_{j,m}} \left(\frac{1}{k} \sum_{i:\frac{i}{n} \in I_{j,m}} \frac{L}{m} \right)^2 dt \\
&= \sum_{j=1}^{m} \int_{I_{j,m}} \left(\frac{L}{m} \right)^2 dt \\
&= \sum_{j=1}^{m} \frac{1}{m} \left(\frac{L}{m} \right)^2 = \left(\frac{L}{m} \right)^2 .
\end{aligned}
$$

The above implies that $\| f^* - f_n \|^2 \to 0$ as $n \to \infty$, since $m = m_n \to \infty$ as $n \to \infty$. In words, with n sufficiently large we can approximate f^* to arbitrary accuracy using models in $\mathscr{F}_n$ (even if the functions we are using to approximate f^* are not Lipschitz!).

For any $f \in \mathscr{F}_n$, $f = \sum_{j=1}^{m} c_j \mathbf{1}_{\{t \in I_{j,m}\}}$, we have

Equation:

$$\widehat{R}_n(f) = \frac{1}{n}\sum_{j=1}^{m}\left(\sum_{i:\frac{i}{n}\in I_{j,m}}(c_j - Y_i)^2\right).$$

Let $\widehat{f}_n = \text{argmin}_{f\in\mathscr{F}_n}\ \widehat{R}_n(f)$. Then
Equation:

$$\widehat{f}_n(t) = \sum_{j=1}^{m}\hat{c}_j\,\mathbf{1}_{\{t\in I_{j,m}\}}, \quad \text{where} \quad \hat{c}_j = \frac{1}{k}\sum_{i:\frac{i}{n}\in I_{j,m}} Y_i$$

Example:
Exercise 2
Show [link].
Note that $E\left[\hat{c}_j\right] = c_j^*$ and therefore $E\left[\widehat{f}_n(t)\right] = f_n(t)$. Lets analyze now the expected risk of $\widehat{f}_n$:
Equation:

$$\begin{aligned} E\left[\| f^* - \widehat{f}_n \|^2\right] &= E\left[\| f^* - f_n + f_n - \widehat{f}_n \|^2\right] \\ &= \| f^* - f_n \|^2 + E[\| f_n - \widehat{f}_n \|^2] + 2E\left[\left\langle f^* - f_n, f_n - \widehat{f}_n \right\rangle\right] \\ &= \| f^* - f_n \|^2 + E[\| f_n - \widehat{f}_n \|^2] + 2\left\langle f^* - f_n, E\left[f_n - \widehat{f}_n\right]\right\rangle \\ &= \| f^* - f_n \|^2 + E[\| f_n - \widehat{f}_n \|^2], \end{aligned}$$

where the final step follows from the fact that $E\left[\widehat{f}_n(t)\right] = f_n(t)$. A couple of important remarks pertaining the right-hand-side of equation [link]: The first term, $\| f^* - f_n \|^2$, corresponds to the approximation error, and indicates how well can we approximate the function f^* with a function from $\mathscr{F}_n$. Clearly, the larger the class $\mathscr{F}_n$ is, the smallest we can make this term. This term is precisely the squared bias of the estimator $\widehat{f}_n$. The second term, $E\left[\| f_n - \widehat{f}_n \|^2\right]$, is the estimation error, the variance of our estimator. We will see that the estimation error is small if the class of possible estimators $\mathscr{F}_n$ is also small.
The behavior of the first term in [link] was already studied. Consider the other term:
Equation:

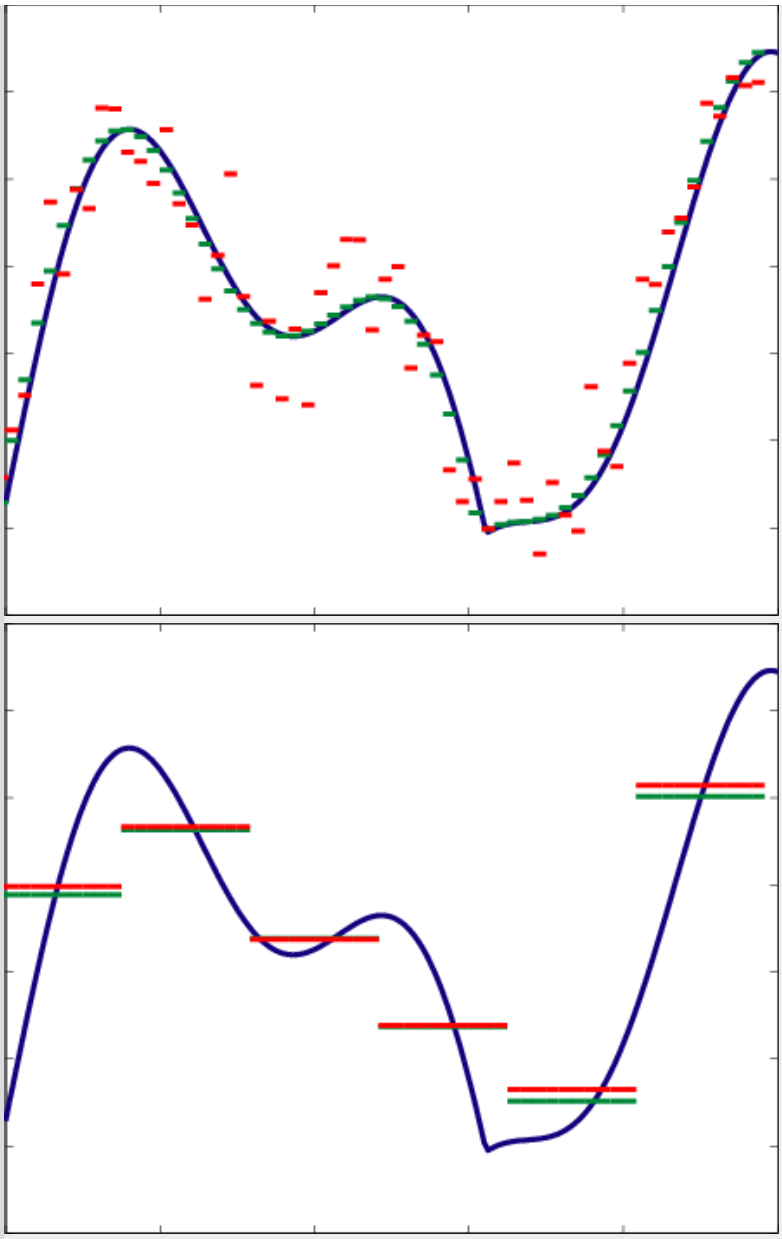
$$
\begin{aligned}
E\left[\| f_n - \widehat{f}_n \|^2\right] &= E\left[\int_0^1 \left|f_n(t) - \widehat{f}_n(t)\right|^2 dt\right] \\
&= E\left[\sum_{j=1}^{m} \int_{I_{j,m}} \left|c_j^* - \hat{c}_j\right|^2 dt\right] \\
&= \sum_{j=1}^{m} \int_{I_{j,m}} E[|c_j^* - \hat{c}_j|^2]\, dt \\
&= \sum_{j=1}^{m} \int_{I_{j,m}} \frac{E\left[W^2\right]}{k}\, dt \\
&\leq \sum_{j=1}^{m} \int_{I_{j,m}} \frac{\sigma^2}{k}\, dt \\
&= \sum_{j=1}^{m} \frac{1}{m}\frac{\sigma^2}{k} = \frac{\sigma^2}{k} = \frac{m}{n}\sigma^2
\end{aligned}
$$

Combining all the facts derived we have
Equation:

$$
E[\| f^* - \widehat{f}_n \|^2] \leq \frac{L^2}{m^2} + \frac{m}{n}\sigma^2 = O\left(\max\left\{\frac{1}{m^2}, \frac{m}{n}\right\}\right).
$$

This equation used Big-O notation.
What is the best choice of m? If m is small then the approximation error (**i.e.,** $O\left(1/m^2\right)$) is going to be large, but the estimation error (**i.e.,** $O(m/n)$) is going to be small, and vice-versa. This two conflicting goals provide a tradeoff that directs our choice of m (as a function of n). In [link] we depict this tradeoff. In [link](a) we considered a large m_n value, and we see that the approximation of f^* by a function in the class $\mathscr{F}_n$ can be very accurate (that is, our estimate will have a small bias), but when we use the measured data our estimate looks very bad (high variance). On the other hand, as illustrated in [link](b), using a very small m_n allows our estimator to get very close to the best approximating function in the class $\mathscr{F}_n$, so we have a low variance estimator, but the bias of our estimator (**i.e.,** the difference between f_n and f^*) is quite considerable.

Approximation and estimation of f^* (in blue) for $n = 60$. The function f_n is depicted in green and the function $\widehat{f}_n$ is depicted in red. In (a)we have $m = 60$ and in (b) we have $m = 6$.



We need to balance the two terms in the right-hand-side of [link] in order to maximize the rate of decay (with n) of the expected risk. This implies that $\frac{1}{m^2} = \frac{m}{n}$ therefore $m_n = n^{1/3}$ and the Mean Squared Error (MSE) is

Equation:

$$E[\| f_n - \widehat{f}_n \|^2] = O\left(n^{-2/3}\right).$$

So the sieve $\mathscr{F}_1, \mathscr{F}_2, \cdots$ with

Equation:

$$\mathscr{F}_n = \left\{ f : f(t) = \sum_{j=1}^{m_n} c_j \, \mathbf{1}_{\left\{ \frac{j-1}{m_n} \leq t < \frac{j}{m_n} \right\}}, \;\; c_j \in \mathbf{R} \right\},$$

produces a $\mathscr{F}$-consistent estimator for $f^* = E[Y|X+x] \in \mathscr{F}$.
It is interesting to note that the rate of decay of the MSE we obtain with this strategy cannot be further improved by using more sophisticated estimation techniques (that is, $n^{-2/3}$ is the **minimax** MSE rate for this problem). Also, rather surprisingly, we are considering classes of models $\mathscr{F}_n$ that are actually not Lipschitz, therefore our estimator of f^* is not a Lipschitz function, unlike f^* itself.

Plug-In Classifier and Histogram Classifier

We return to the topic of classification, and we assume an input (feature) space $\mathscr{X}$ and a binary output (label) space $\mathscr{Y} = \{0, 1\}$. Recall that the Bayes classifier (which minimizes the probability of misclassification) is defined by
Equation:

$$f^*(x) = \begin{cases} 1, & P(Y = 1|X = x) \geq 1/2 \\ 0, & otherwise \end{cases}.$$

Throughout this section, we will denote the conditional probability function by
Equation:

$$\eta(x) \equiv P(Y = 1|X = x).$$

Plug-in Classifiers

One way to construct a classifier using the training data $\{X_i, Y_i\}_{i=1}^n$ is to estimate $\eta(x)$ and then plug-it into the form of the Bayes classifier. That is obtain an estimate,
Equation:

$$\hat{\eta}_n(x) = \eta\left(x; \{X_i, Y_i\}_{i=1}^n\right)$$

and then form the “plug-in" classification rule
Equation:

$$\widehat{f}(x) = \begin{cases} 1, & \hat{\eta}(x) \geq 1/2 \\ 0, & otherwise \end{cases}.$$

Note: The function $\eta(x)$ is generally more complicated than the ultimate classification rule (binary-valued), as we can see

Equation:

$$\begin{array}{rcl} \eta & : & \mathscr{X} \to [0, 1] \\ f & : & \mathscr{X} \to \{0, 1\} \end{array}.$$

Therefore, in this sense plug-in methods are solving a more complicated problem than necessary. However, plug-in methods can perform well, as demonstrated by the next result.
Theorem
Plug-in Classifier

Let $\tilde{\eta}$ be an approximation to η, and consider the plug-in rule
Equation:

$$f(x) = \begin{cases} 1, & \tilde{\eta}(x) \geq 1/2 \\ 0, & otherwise \end{cases}.$$

Then,
Equation:

$$R(f) - R^* \leq 2E[|\eta(x) - \tilde{\eta}(x)|]$$

where
Equation:

$$\begin{aligned} R(f) &= P(f(X) \neq Y) \\ R^* &= R\left(f^*\right) = \inf_f R(f) \end{aligned}.$$

Consider any $x \in \mathbf{R}^d$. In proving the optimality of the Bayes classifier f^* in Lecture 2, we showed that
Equation:

$$P(f(x) \neq Y | X = x) - P\Big(f^*(x) \neq Y | X = x\Big) = (2\eta(x) - 1)\Big[\mathbf{1}_{\{f^*(x)=1\}} - \mathbf{1}_{\{f(x)=1\}}\Big],$$

which is equivalent to
Equation:

$$P(f(x) \neq Y | X = x) - P\Big(f^*(x) \neq Y | X = x\Big) = |2\eta(x) - 1| \, \mathbf{1}_{\{f^*(x) \neq f(x)\}},$$

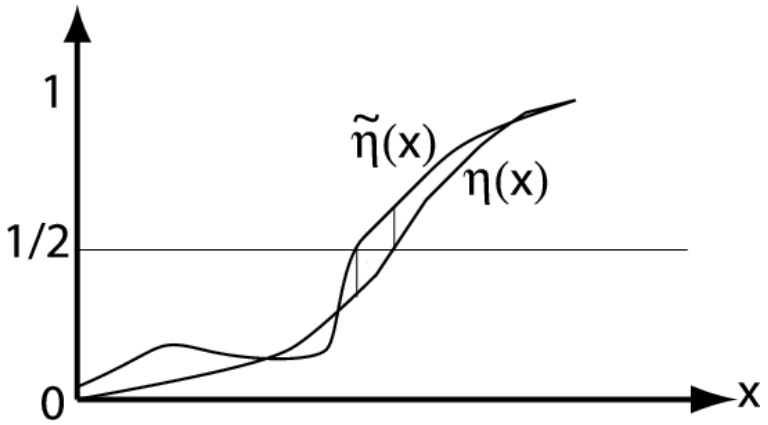
since $f^*(x) = 1$ whenever $2\eta(x) - 1 > 0$. Thus,
Equation:

$$\begin{aligned} P(f(X) \neq Y) - R^* &= \int_{\mathbf{R}^d} 2|\eta(x) - 1/2| \, \mathbf{1}_{\{f^*(x) \neq f(x)\}} p_X(x) dx \\ &\quad \text{where } p_X(x) \text{ is the marginal density of } X \\ &\leq \int_{\mathbf{R}^d} 2|\eta(x) - \tilde{\eta}(x)| \mathbf{1}_{\{f^*(x) \neq f(x)\}} p_X(x) dx \\ &\leq \int_{\mathbf{R}^d} 2|\eta(x) - \tilde{\eta}(x)| p_X(x) dx \\ &= 2E[|\eta(X) - \tilde{\eta}(X)|] \end{aligned}$$

where the first inequality follows from the fact
Equation:

$$f(x) \neq f^*(x) \;\; \Rightarrow \;\; |\eta(x) - \tilde{\eta}(x)| \geq |\eta(x) - 1/2|$$

and the second inequality is simply a result of the fact that $\mathbf{1}_{\{f^*(x) \neq f(x)\}}$ is either 0 or 1.



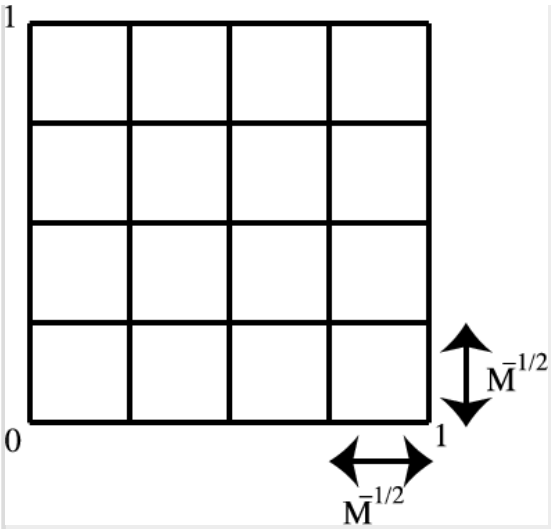
Pictorial illustration of $|\eta(x) - \tilde{\eta}(x)| \geq |\eta(x) - 1/2|$ when $f(x) \neq f^*(x)$. Note that the inequality $P(f(X) \neq Y) - R^* \leq \int_{\mathbf{R}^d} 2|\eta(x) - \tilde{\eta}(x)| \mathbf{1}_{\{f^*(x) \neq f(x)\}} p_X(x) dx$ shows that the excess risk is at most twice the integral over the set where $f^*(x) \neq f(x)$. The difference $|\eta(x) - \tilde{\eta}(x)|$ may be arbitrarily large away from this set without effecting the error rate of the classifier. This illustrates the fact that estimating η well everywhere (i.e., regression) is unnecessary for the design of a good classifier (we only need to determine where η crosses the $1/2$-level). In other words, "classification is easier than regression."

The theorem shows us that a good estimate of η can produce a good plug-in classification rule. By "good" estimate, we mean an estimator $\tilde{\eta}$ that is close to η in expected L_1-norm.

The Histogram Classifier

Let's assume that the (input) features are randomly distributed over the unit hypercube $\mathscr{X} = [0,1]^d$ (note that by scaling and shifting any set of bounded features we can satisfy this assumption), and assume that the (output) labels are binary, i.e., $\mathscr{Y} = \{0,1\}$. A histogram classifier is based on a partition the hypercube $[0,1]^d$ into M smaller cubes of equal size.

Example:
Partition of hypercube in 2 dimensions
Consider the unit square $[0,1]^2$ and partition it into M subsquares of equal area (assuming M is a squared integer). Let the subsquares be denoted by $\{Q_i\},\ i = 1, ..., M$.



Example of hypercube $[0,1]^2$ in M equally sized partition

Define the following piecewise-constant estimator of $\eta(x)$:
Equation:

$$\hat{\eta}_n(x) = \sum_{j=1}^{M} \widehat{P}_j \mathbf{1}_{\{x \in Q_j\}}$$

where
Equation:

$$\widehat{P}_j = \frac{\sum_{i=1}^{n} \mathbf{1}_{\{X_i \in Q_j, Y_i = 1\}}}{\sum_{i=1}^{n} \mathbf{1}_{\{X_i \in Q_j\}}}.$$

Like our previous denoising examples, we expect that the bias of $\hat{\eta}_n$ will decrease as M increases, but the variance will increase as M increases.

Theorem
Consistency of Histogram Classifiers

If $M \to \infty$ and $\frac{n}{M} \to \infty$ as $n \to \infty$, then the histogram classifier risk converges to the Bayes risk for every distribution P_{XY} with marginal density $p_X(x) \geq c$, for some constant $c > 0$.[footnote].
Actually, the result holds for every distribution P_{XY}. For the more general theorem, refer to Theorem 6.1 in **A probabilistic Theory of Pattern Recognition** by Luc Devroye, László Györfi and Gábor Lugosi.

What the theorem tells us is that we need the number of partition cells to tend to infinity (to insure that the bias tends to zero), but they can't grow faster than the number of samples (**i.e.,** we want the number of samples per box tending to infinity to drive the variance to zero).

Let $P_j \equiv \frac{\int_{Q_j} \eta(x) p_X(x) dx}{\int_{Q_j} p_X(x) dx}$ (the theoretical analog of $\widehat{P}_j$) and define

Equation:

$$\overline{\eta}(x) = \sum_{j=1}^{M} P_j \mathbf{1}_{\{x \in Q_j\}}$$

The function $\overline{\eta}$ is the theoretical analog of $\hat{\eta}$ (i.e., the function obtained by averaging η over the partition cells). By the triangle inequality,
Equation:

$$E\big[\big|\hat{\eta}_n(X) - \eta(X)\big|\big] \;\le\; \underbrace{E\big[\big|\hat{\eta}_n(X) - \overline{\eta}(X)\big|\big]}_{EstimationError} \;+\; \underbrace{E\big[\big|\overline{\eta}_n(X) - \eta(X)\big|\big]}_{ApproximationError}$$

Let's first bound the estimation error. For any $x \in [0,1]^d$, let $Q(x)$ denote the histogram bin in which x falls in. Define the random variable
Equation:

$$N(x) = \sum_{i=1}^{n} \mathbf{1}_{\{X_i \in Q(x)\}}$$

If $Q(x) = Q_j$, then this random variable is simply $n\widehat{P}_j$. Note that
Equation:

$$\hat{\eta}_n(x) = \frac{1}{N(x)} B(x)$$

where $B(x) == \sum_{i=1}^{n} \mathbf{1}_{\{X_i \in Q(x),\, Y_i = 1\}} = \sum_{i:X_i \in Q(x)} Y_i$. $B(x)$ is simply the number of samples in cell $Q(x)$ labelled 1. Now $\hat{\eta}_n(x)$ is a fairly complicated random variable, but the conditional distribution of $B(x)$ given $N(x)$ is relatively simple. Note that
Equation:

$$B(x) \,|\, N(x) = k \;\sim\; \text{Binomial}(k, \overline{\eta}(x))$$

since $\overline{\eta}(x)$ is the probability of a sample in $Q(x)$ having the label 1 and we are conditioning on the event of observing k samples in $Q(x)$.

Now consider the conditional expectation
Equation:

$$E\big[\big|\hat{\eta}_n(x) - \overline{\eta}(x)\big| \mid N(x) = k\big] \;\le\; \begin{cases} E\Big[\Big|\frac{B(x)}{N(x)} - \overline{\eta}(x)\Big| \mid N(x) = k\Big], & k > 0 \\ 1, & k = 0 \quad (\text{since } 0 \le \overline{\eta}(x) \le 1) \end{cases}$$

Next note that
Equation:

$$\begin{aligned} E\left[\left|\frac{B(x)}{N(x)}-\overline{\eta}\left(x\right)\right| \mid N\left(x\right)=k\right] &= E\left[\left|\frac{B(x)}{k}-\overline{\eta}\left(x\right)\right| \mid N\left(x\right)=k\right] \\ &= E\left[\frac{1}{k}\left|B\left(x\right)-\underbrace{k\overline{\eta}\left(x\right)}_{E[B(x)]}\right| \mid N\left(x\right)=k\right] \\ &\leq \frac{1}{k}\left(\underbrace{E\left[\left|B\left(x\right)-k\overline{\eta}(x)\right|^{2} \mid N\left(x\right)=k\right]}_{\text{conditional variance of } B(x)}\right)^{\frac{1}{2}} \end{aligned}$$

by the Jensen's inequality, $E\left[\left|Z\right|\right] \leq (E[\left|Z\right|^{2}])^{\frac{1}{2}}$.

Therefore,
Equation:

$$\begin{aligned} E\left[\left|\frac{B(x)}{N(x)}-\overline{\eta}\left(x\right)\right| \mid N\left(x\right)=k\right] &\leq \frac{1}{k}(k\overline{\eta}\left(x\right)\left(1-\overline{\eta}\left(x\right)\right))^{\frac{1}{2}} \\ &= \sqrt{\frac{\overline{\eta}\left(x\right)\left(1-\overline{\eta}\left(x\right)\right)}{k}} \end{aligned}$$

and
Equation:

$$E\left[\left|\hat{\eta}_{n}\left(x\right)-\overline{\eta}\left(x\right)\right| \mid N\left(x\right)=k\right] \leq \begin{cases} \sqrt{\frac{\overline{\eta}(x)(1-\overline{\eta}(x)}{k}}, & k>0 \\ 1, & k=0 \end{cases}$$

or in other words,
Equation:

$$E\left[\left|\hat{\eta}_{n}\left(x\right)-\overline{\eta}\left(x\right)\right| \mid N\left(x\right)=k\right] \leq \sqrt{\frac{\overline{\eta}\left(x\right)(1-\overline{\eta}\left(x\right)}{N(x)}}\mathbf{1}_{\{N(x)>0\}} + \mathbf{1}_{\{N(x)=0\}}$$

Now taking expectation with respect to $N(x)$
Equation:

$$\begin{aligned} E_{N}\left[E\left[\left|\hat{\eta}_{n}\left(x\right)-\overline{\eta}\left(x\right)\right|N\left(x\right)=k\right]\right] &\leq E_{N}\left[\sqrt{\frac{\overline{\eta}\left(x\right)(1-\overline{\eta}\left(x\right)}{N(x)}}\mathbf{1}_{\{N(x)>0\}}\right] + P\left(N\left(x\right)=0\right) \\ &\leq E\left[\frac{1}{2\sqrt{N(x)}}\mathbf{1}_{\{N(x)>0\}}\right] + P\left(N\left(x\right)=0\right) \\ &\leq \frac{1}{2}P\left(N\left(x\right)\leq k\right) + \frac{1}{2\sqrt{k}}\underbrace{P(N(x)>k)}_{\leq 1} + P\left(N\left(x\right)=0\right) \end{aligned}$$

Now a key fact is that for any $k > 0$, $P(N \leq k) \to 0$ as $n \to \infty$. This follows from the assumption that the marginal density $p_X(x) \geq c$, for some constant $c > 0$, and $\frac{n}{M} \to \infty$ as $n \to \infty$. This result is easily verified by contradiction. If $P(N \leq k) \to q > 0$ as $n \to \infty$, then $P_X(x) > 0$ is contradicted. Thus, for any $\epsilon > 0$ there exists a $k > 0$ such that $\frac{1}{2\sqrt{k}} < \epsilon$ and $P(N \leq k) < \epsilon$ for n sufficiently large. Therefore, for n sufficiently large and every $x \in [0,1]^d$,
Equation:

$$E\left[\left|\hat{\eta}_n(x) - \overline{\eta}(x)\right|\right] < 3\epsilon$$

where the expectation is with respect to the distribution of the sample $\{X_i, Y_i\}_{i=1}^n$. Thus,
Equation:

$$E\left[\left|\hat{\eta}_n(X) - \overline{\eta}(X)\right|\right] \;<\; 3\epsilon$$

where the expectation is now with respect to the distribution of the sample and the marginal distribution of X.

Next consider the approximation error $E[|\overline{\eta}_n(X) - \eta(X)|]$, where the expectation is over X alone. The function η may not itself be continuous, but there is another function η_ϵ that is uniformly continuous and such that $E[|\eta_\epsilon(X) - \eta(X)|] < \epsilon$. Recall that uniformly continuous functions can be well approximated by piecewise constant functions.

By the triangle inequality,
Equation:

$$E[|\overline{\eta} - \eta|] \leq \underbrace{E[|\overline{\eta} - \overline{\eta}_\epsilon|]}_{\leq \epsilon} + E[|\overline{\eta}_\epsilon - \eta_\epsilon|] + \underbrace{E[|\eta_\epsilon - \eta|]}_{\leq \epsilon \text{ by design}}$$

where $\overline{\eta}_\epsilon(x) = \sum_{j=1}^m \left[\int_{Q_j} \eta_\epsilon(x') p_X(x') dx'\right] \mathbf{1}_{\{x \in Q_j\}}$.
Equation:

$$\begin{aligned} E[|\overline{\eta}(X) - \overline{\eta}_\epsilon(X)|] &= \sum_{j=1}^m \left[\int_{Q_j} |\eta(x) - \eta_\epsilon(x)| p_X(x) dx\right] \mathbf{1}_{\{x \in Q_j\}} \\ &\leq \epsilon \end{aligned}$$

and since η_ϵ is uniformly continuous,
Equation:

$$\begin{aligned} E[|\overline{\eta}_\epsilon(X) - \eta_\epsilon(X)|] &= \sum_{j=1}^M \int_{Q_j} |\overline{\eta}_\epsilon(x) - \eta_\epsilon(x)| \mathbf{1}_{\{x \in Q_j\}} p_X(x) dx \\ &\leq \sum_{j=1}^M \delta \, P(x \in Q_j), \qquad \text{where } \delta \text{ depends on } M \\ &= \delta, \qquad\qquad\qquad\qquad \text{since } \sum_{j=1}^M P(X \in Q_j) = 1 \end{aligned}$$

By taking M sufficiently large, δ can be made arbitrarily small. So for large M, $\delta \leq \epsilon$.

Thus, we have shown
Equation:

$$E[|\overline{\eta}(X) - \eta(X)|] < 3\epsilon$$

for sufficiently large M. Since $\epsilon > 0$ was arbitrary, we have shown that taking
Equation:

$$\widehat{f}_n(x) = \begin{cases} 1, & \hat{\eta}_n(x) \geq 1/2 \\ \\ 0, & otherwise \end{cases}$$

satisfies
Equation:

$$P\left(\widehat{f}_n(X) \neq Y\right) - P\left(f^*(X) \neq Y\right) \;\leq\; 2E\left[\left|\hat{\eta}_n(X) - \eta(X)\right|\right] \to 0$$

if
Equation:

$$\begin{aligned} M &\to \infty \\ \frac{n}{M} &\to \infty \text{ as } n \to \infty \end{aligned}$$

Note: $P\left(\widehat{f}_n(X) \neq Y\right) = E\left[\mathbf{1}_{\left\{\widehat{f}(X) \neq Y\right\}}\right]$ is the expected risk of $\widehat{f}$, with expectation over the distributions of (X, Y) and $\{X_i, Y_i\}_{i=1}^n$.

Probably Approximately Correct (PAC) Learning

Introduction

Overview of the Learning Problem

The fundamental problem in learning from data is proper Model Selection. As we have seen in the previous lectures, a model that is too complex could overfit the training data (causing an estimation error) and a model that is too simple could be a bad approximation of the function that we are trying to estimate (causing an approximation error). The estimation error arises because of the fact that we do not know the true joint distribution of data in the input and output space, and therefore we minimize the empirical risk (which, for each candidate model, is a random number depending on the data) and estimate the average risk again from the limited number of training samples we have. The approximation error measures how well the functions in the chosen model space can approximate the underlying relationship between the output space on the input space, and in general improves as the "size" of our model space increases.

Lecture Outline

In the preceding lectures, we looked at some solutions to deal with the overfitting problem. The basic approach followed was the Method of Sieves, in which the complexity of the model space was chosen as a function of the number of training samples. In particular, both the denoising and classification problems we looked at consider estimators based on histogram partitions. The size of the partition was an increasing function of the number of training samples. In this lecture, we will refine our learning methods further introduce model selection procedures that automatically adapt to the distribution of the training data, rather than basing the model class solely on the number of samples. This sort of adaptivity will play a major role in the design of more effective classifiers and denoising methods. The key to designing data-adaptive model selection procedures is obtaining useful upper bounds on the estimation error. To this end, we will introduce the idea of "Probably Approximately Correct" learning methods.

Recap: Method of Sieves

The method of Sieves underpinned our approaches in the denoising problem and in the histogram classification problem. Recall that the basic idea is to define a sequence of model spaces $\mathscr{F}_1$, $\mathscr{F}_2$, ...of increasing complexity, and then given the training data $\{X_i, Y_i\}_{i=1}^n$ select a model according to

Equation:

$$\widehat{f_n} = \arg\min_{f \in \mathscr{F}_n} \widehat{R}_n(f).$$

The choice of the model space $\mathscr{F}_n$ (and hence the model complexity and structure) is determined completely by the sample size n, and does not depend on the (empirical) distribution of training data. This is a major limitation of the sieve method. In a nutshell, the method of sieves tells us to average the data in a certain way (e.g., over a partition of $\mathscr{X}$) based on the sample size, independent on the sample values themselves.

In general, learning basically comprises of two things:

1. Averaging data to reduce variability
2. Deciding **where (or how)** to average

Sieves basically force us to deal with (2) **a priori** (before we analyze the training data). This will lead to suboptimal classifiers and estimators, in general. Indeed deciding where/how to average is the really interesting and fundamental aspect of learning; once this is decided we have effectively solved the learing problem. There are at least two possibilities for breaking the rigidity of the method of sieves, as we shall see in the following section.

Data Adaptive Model Spaces

Structural Risk Minimization (SRM)

The basic idea is to select $\mathscr{F}_n$ based on the training data themselves. Let $\mathscr{F}_1$, $\mathscr{F}_2$, ...be a sequence of model spaces of increasing sizes/complexities with
Equation:

$$\lim_{k \to \infty} \inf_{f \in \mathscr{F}_k} R(f) = R^*.$$

Let
Equation:

$$\widehat{f}_{n,k} = \arg\min_{f \in \mathscr{F}_k} \widehat{R}_n(f)$$

be a function from $\mathscr{F}_k$ that minimizes the empirical risk. This gives us a sequence of selected models $\widehat{f}_{n,1}, \widehat{f}_{n,2}, \cdots$ Also associate with each set $\mathscr{F}_k$ a value $C_{n,k} > 0$ that measures the complexity or “size” of the set $\mathscr{F}_k$. Typically, $C_{n,k}$ is monotonically

increasing with k (since the sets are of increasing complexity) and decreasing with n (since we become more confident with more training data). More precisely, suppose that the $C_{n,k}$ chosen so that

Equation:

$$P\left(\sup_{f\in\mathscr{F}_k}\left|\widehat{R}_n\left(f\right)-R\left(f\right)\right|>C_{n,k}\right)<\delta$$

for some small $\delta>0$. Then we may conclude that with very high probability (at least $1-\delta$) the empirical risk $\widehat{R}_n$ is within $C_{n,k}$ of R uniformly on the class $\mathscr{F}_k$. This type of bound suffices to bound the estimation error (variance) of the model selection process of the form $R\left(f\right)\leq\widehat{R}_n\left(f\right)+C_{n,k}$, and SRM selects the final model by minimizing this bound over all functions in $\bigcup_{k\geq1}\mathscr{F}_k$. The selected model is given by $\widehat{f}_{n,\widehat{k}}$, where

Equation:

$$\widehat{k}=\operatorname*{argmin}_{k\geq1}\left\{\widehat{R}_n\left(\widehat{f}_{n,k}\right)+C_{n,k}\right\}.$$

A typical example could be the use of VC dimension to characterize the complexity of the collection of model spaces **i.e.,**$C_{n,k}$ is derived from a bound on the estimation error.

Complexity Regularization

Consider a very large class of candidate models $\mathscr{F}$. To each $f\in\mathscr{F}$ assign a complexity value $C_n\left(f\right)$. Assume that the complexity value is chosen so that

Equation:

$$P\left(\sup_{f\in\mathscr{F}}\left|\widehat{R}_n\left(f\right)-R\left(f\right)\right|>C_n\left(f\right)\right)<\delta.$$

This probability bound also implies an upper bound on the estimation error and complexity regularization is based on the criterion

Equation:

$$\widehat{f}_n=\operatorname*{argmin}_{f\in\mathscr{F}}\left\{\widehat{R}_n\left(f\right)+C_n\left(f\right)\right\}.$$

Complexity Regularization and SRM are very similar and equivalent in certain instances. A distinguishing feature of SRM and complexity requlariza tion techniques is that the complexity and structure of the model is not fixed prior to examining the data; the data aid in the selection of the best complexity. In fact, the key difference compared to the Method of Sieves is that these techniques can allow the data to play an integral role in deciding where and how to average the data.

Probably Approximately Correct (PAC) learning

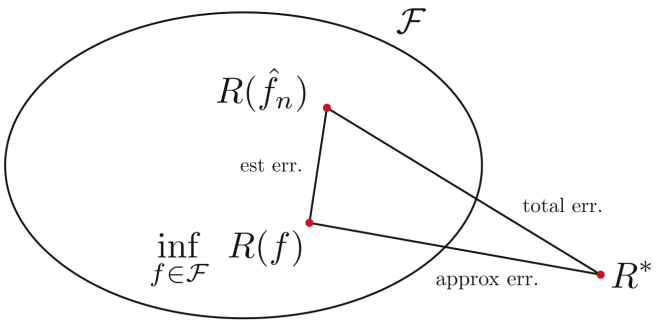
Probability bounds of the forms in [link] and [link] are the foundation for SRM and complexity regularization techniques. The simplest of these bounds are known as PAC bounds in the machine learning community.

Approximation and Estimation Errors

In order to develop complexity regularization schemes we will need to revisit the estimation error / approximation error trade-off. Let $\widehat{f}_n = \operatorname{argmin}_{f \in \mathscr{F}} \widehat{R}_n(f)$ for some space of models $\mathscr{F}$.
Equation:

$$R\left(\widehat{f}_n\right) - R^* = \underbrace{R\left(\widehat{f}_n\right) - \inf_{f \in \mathscr{F}} R(f)}_{\text{estimation Error}} + \underbrace{\inf_{f \in \mathscr{F}} R(f) - R^*}_{\text{approximation error}}$$

The approximation error depends on how close f^* is close to $\mathscr{F}$, and without making assumptions, this is unknown. The estimation error is quantifiable, and depends on the complexity or size of $\mathscr{F}$. The error decomposition is illustrated in [link]. The estimation error quantifies how much we can “trust” the empirical risk minimization process to select a model close to the best in a given class.



Relationship between the errors

Probability bounds of the forms in [link] and [link] guarantee that the empirical risk is uniformly close to the true risk, and using [link] and [link] it is possible to show that with high probability the selected model $\widehat{f}_n$ satisfies
Equation:

$$R\left(\widehat{f}_n\right) - \inf_{f \in \mathscr{F}_k} R(f) \leq C(n,k)$$

or
Equation:

$$R\left(\widehat{f}_n\right) - \inf_{f \in \mathscr{F}_k} R(f) \leq C_n(f).$$

The PAC Learning Model

The estimation error will be small if $R\left(\widehat{f}_n\right)$ is close to $\inf_{f \in \mathscr{F}} R(f)$. PAC learning expresses this as follows. We want $\widehat{f}_n$ to be a "probably approximately correct" (PAC) model from $\mathscr{F}$. Formally, we say that $\widehat{f}_n$ is ε accurate with confidence $1-\delta$, or $(\varepsilon, \delta)-$ PAC for short, if
Equation:

$$P\left(R\left(\widehat{f}_n\right) - \inf_{f \in \mathscr{F}} R(f) > \varepsilon\right) < \delta.$$

This says that the difference between $R\left(\widehat{f}_n\right)$ and $\inf_{f\in\mathscr{F}} R(f)$ is greater than ε with probability less than δ. Sometimes, especially in the machine learning community, PAC bounds are stated as, "with probability of at least $1-\delta$, $|R\left(\widehat{f}_n\right) - \inf_{f\in\mathscr{F}} R(f)| \leq \varepsilon$"

To introduce PAC bounds, let us consider a simple case. Let $\mathscr{F}$consist of a finite number of models, and let $|\mathscr{F}|$ denote that number. Furthermore, assume that $\min_{f\in\mathscr{F}} R(f) = 0$.

Example:
$\mathscr{F}$= set of all histogram classifiers with M bins $\Rightarrow |\mathscr{F}| = 2^M$.
Equation:

$$\min_{f\in\mathscr{F}} R(f) = 0 \Rightarrow \exists \text{ a classifier in } \mathscr{F} \text{ that has a zero probability of error}$$

Theorem

Assume $|\mathscr{F}| < \infty$ and $\min_{f\in\mathscr{F}} R(f) = 0$, where $R(f) = P(f(X) \neq Y)$. Let $\widehat{f}_n = \text{argmin}_{f\in\mathscr{F}} \widehat{R}_n(f)$, where $\widehat{R}_n(f) = \frac{1}{n}\sum_{i=1}^{n} \mathbf{1}_{\{f(X_i)\neq Y_i\}}$. Then for every n and $\varepsilon > 0$,
Equation:

$$P\left(R\left(\widehat{f}_n\right) > \varepsilon\right) \;\leq\; |\mathscr{F}| e^{-n\varepsilon} \;\equiv\; \delta.$$

Since $\min_{f\in\mathscr{F}} R(f) = 0$, it follows that $\widehat{R}_n\left(\widehat{f}_n\right) = 0$. In fact, there may be several $f \in \mathscr{F}$ such that $\widehat{R}_n(f) = 0$. Let $\mathscr{G} = \left\{f : \widehat{R}_n(f) = 0\right\}$.
Equation:

$$
\begin{aligned}
P\left(R\left(\widehat{f}_n\right) > \varepsilon\right) &\leq P\left(\bigcup_{f \in \mathscr{G}} \{R(f) > \varepsilon\}\right) \\
&= P\left(\bigcup_{f \in \mathscr{F}} \left\{R(f) > \varepsilon,\ \widehat{R}_n(f) = 0\right\}\right) \\
&= P\left(\bigcup_{f \in \mathscr{F}: R(f) > \varepsilon} \left\{\widehat{R}_n(f) = 0\right\}\right) \\
&\leq \sum_{f \in \mathscr{F}: R(f) > \varepsilon} P\left(\widehat{R}_n(f) = 0\right) \\
&\leq |\mathscr{F}| . (1-\varepsilon)^n
\end{aligned}
$$

The last inequality follows from the fact that if $R(f) = P(f(X) \neq Y) > \varepsilon$, then the probability that n i.i.d. samples will satisfy $f(X) = Y$ is less than or equal to $(1-\varepsilon)^n$. Note that this is simply the probability that $\widehat{R}_n(f) = \frac{1}{n}\sum_{i=1}^{n} \mathbf{1}_{\{f(X_i) \neq Y_i\}} = 0$. Finally apply the inequality $1 - x \leq e^{-x}$ to obtain the desired result.

Note that for n sufficiently large, $\delta = |\mathscr{F}| e^{-n\varepsilon}$ is arbitrarily small. To achieve a (ε, δ)-PAC bound for a desired $\varepsilon > 0$ and $\delta > 0$ we require at least $n = \frac{\log|\mathscr{F}| - \log\delta}{\varepsilon}$ training examples.

Corollary

Assume that $|\mathscr{F}| < \infty$ and $\min_{f \in \mathscr{F}} R(f) = 0$. Then for every n

Equation:

$$
E\left[R\left(\widehat{f}_n\right)\right] \leq \frac{1 + \log|\mathscr{F}|}{n}.
$$

Recall that for any non-negative random variable Z with finite mean,
$E[Z] = \int_0^\infty P(Z > t) dt$. This follows from an application of integration by parts.

Equation:

$$
\begin{aligned}
E\Big[R\left(\widehat{f}_n\right)\Big] &= \int_0^\infty P\left(R\left(\widehat{f}_n\right) > t\right) dt \\
&= \int_0^u \underbrace{P\Big(R\left(\widehat{f}_n\right) > t\Big)}_{\leq 1} dt + \int_u^\infty P\left(R\left(\widehat{f}_n\right) > t\right) dt, \quad \text{for any } u > 0 \\
&\leq u + |\mathscr{F}| \int_u^\infty e^{-nt} dt \\
&= u + \frac{|\mathscr{F}|}{n} e^{-nu}
\end{aligned}
$$

Minimizing with respect to u produces the smallest upper bound with $u = \frac{\log|\mathscr{F}|}{n}$

Chernoff's Bound and Hoeffding's Inequality

Introduction

Motivation

In the last lecture we consider a learning problem in which the optimal function belonged to a finite class of functions. Specifically, for some collection of functions $\mathscr{F}$with finite cardinality $|\mathscr{F}| \leq \infty$, we have
Equation:

$$\min_{f \in \mathscr{F}} R(f) = 0 \Rightarrow f^* \in \mathscr{F}.$$

This is almost always not the situation in the real-world learning problems. Let us suppose we have a finite collection of candidate functions $\mathscr{F}$. Furthermore, we do not assume that the optimal function f^*, which satisfies
Equation:

$$R\left(f^*\right) = \inf_f R(f)$$

where the $\inf$ is taken over all measurable functions, is a member of $\mathscr{F}$. That is, we make few, if any, assumptions about f^*. This situation is sometimes termed as **Agnostic Learning**. The root of the word agnostic literally means **not known**. The term agnostic learning is used to emphasize the fact that often, perhaps usually, we may have no prior knowledge about f^*. The question then arises about how we can reasonably select an $f \in \mathscr{F}$ in this setting.

The Problem

The PAC style bounds discussed in the previous lecture, offer some help. Since we are selecting a function based on the empirical risk, the question is how close is $\widehat{R}_n(f)$ to $R(f) \forall f \in \mathscr{F}$. In other words, we wish that the empirical risk is a good indicator of the true risk for every function in $\mathscr{F}$. If this is case, the selection of f that minimizes the empirical risk
Equation:

$$\widehat{f_n} = \arg\min_{f \in \mathscr{F}_n} \widehat{R}_n(f)$$

should also yield a small true risk, that is, $R\left(\widehat{f_n}\right)$ should be close to $\min_{f \in \mathscr{F}} R(f)$. Finally, we can thus state our desired situation as
Equation:

$$P\left(\max_{f \in \mathscr{F}_n} \left|\widehat{R_n}(f) - R(f)\right| > \epsilon\right) \; < \; \delta,$$

for small values of ϵ and δ. In other words, with probability at least $1 - \delta$, $\left|\widehat{R_n}(f) - R(f)\right| > \epsilon, \forall f \in \mathscr{F}$.
In this lecture, we will start to develop bounds of this form. First we will focus on bounding

$P\left(\left|\widehat{R_n}\left(f\right) - R\left(f\right)\right| > \epsilon\right)$ for one fixed $f \in \mathscr{F}$.

Developing Initial Bounds

To begin, let us recall the definition of empirical risk for $\{X_i, Y_i\}_{i=1}^n$ be a collection of training data. Then the empirical risk is defined as
Equation:

$$\widehat{R}_n\left(f\right) = \frac{1}{n}\sum_{i=1}^{n} \ell\left(f\left(X_i\right), Y_i\right).$$

Note that since the training data $\{X_i, Y_i\}_{i=1}^n$ are assumed to be **i.i.d.** pairs, the terms in the sum are **i.i.d** random variables.

Let
Equation:

$$L_i = \ell\left(f\left(X_i\right), Y_i\right).$$

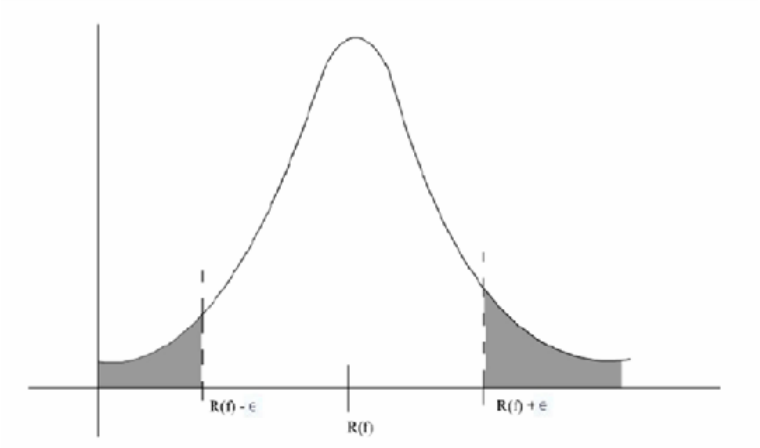
The collection of losses $\{L_i\}_{i=1}^n$ is **i.i.d** according to some unknown distribution (depending on the unknown joint distribution of (X,Y) and the loss function). The expectation of L_i is
$E\left[\ell\left(f\left(X_i\right), Y_i\right)\right] = E\left[\ell\left(f\left(X\right), Y\right)\right] = R\left(f\right)$, the true risk of f. For now, let's assume that f is fixed.
Equation:

$$E\left[\widehat{R_n}\left(f\right)\right] = \frac{1}{n}\sum_{i=1}^{n} E\left[\ell\left(f\left(X_i\right), Y_i\right)\right] = \frac{1}{n}\sum_{i=1}^{n} E\left[L_i\right] = R\left(f\right)$$

We know from the strong law of large numbers that the average (or empirical mean) $\widehat{R_n}\left(f\right)$ converges almost surely to the true mean $R(f)$. That is, $\widehat{R_n}\left(f\right) \to R\left(f\right)$ almost surely as $n \to \infty$. The question is how fast.

Concentration of Measure Inequalities

Concentration inequalities are upper bounds on how fast empirical means converge to their ensemble counterparts, in probability. The area of the shaded tail regions in Figure 1 is $P\left(\left|\widehat{R_n}\left(f\right) - R\left(f\right)\right| > \epsilon\right)$. We are interested in finding out how fast this probability tends to zero as $n \to \infty$.



Distribution of $\widehat{R_n}(f)$

At this stage, we recall **Markov's Inequality**. Let Z be a nonnegative random variable.
Equation:

$$\begin{aligned} E[Z] &= \int_0^\infty zp(z)dz \\ &= \int_0^t zp(z)dz + \int_u^\infty zp(z)dz \\ &\geq 0 + t\int_t^\infty zp(z)dz \\ &= tP(Z \geq t) \\ \Rightarrow P(Z \geq t) &\leq \frac{E[Z]}{t} \\ \Rightarrow P\left(Z^2 \geq t^2\right) &\leq \frac{E\left[Z^2\right]}{t^2} \end{aligned}$$

Take
Equation:

$$Z = |\widehat{R_n(f)} - R(f)| \quad \text{and} \quad t = \epsilon$$

Equation:

$$
\begin{aligned}
P\left(\left|\widehat{R_n}\left(f\right)-R\left(f\right)\right|\geq\epsilon\right) &\leq \frac{E\left[\left|\widehat{R_n\left(f\right)}-R\left(f\right)\right|^2\right]}{\epsilon^2} \\
&\leq \frac{\operatorname{var}\left(\widehat{R}_n\left(f\right)\right)}{\epsilon^2} \\
&= \frac{\sum_{i=1}^{n}\operatorname{var}\left(\frac{L_i}{n}\right)}{\epsilon^2} \\
&= \frac{\operatorname{var}(\ell(X),Y)}{n\epsilon^2} \\
&= \frac{\sigma_L^2}{n\epsilon^2}
\end{aligned}
.
$$

So, the probability goes to zero at a rate of at least n^{-1}. However, it turns out that this is an extremely loose bound. According to the Central Limit Theorem
Equation:

$$
\widehat{R_n}\left(f\right)=\frac{1}{n}\sum_{i=1}^{n}L_i\rightarrow N\left(R\left(f\right),\frac{\sigma_L^2}{n}\right)\quad\text{as}\quad n\rightarrow\infty
$$

in distribution. This suggests that for large values of n,
Equation:

$$
P(|\widehat{R_n}\left(f\right)-R\left(f\right)|\geq\epsilon)\approx O\left(e^{-\frac{n\epsilon^2}{2\sigma_L^2}}\right).
$$

That is, the Gaussian tail probability is tending to zero exponentially fast.

Chernoff's Bound

Note that for any nonnegative random variable Z and $t>0$,
Equation:

$$
P\left(Z\geq t\right)=P\left(e^{sZ}\geq e^{st}\right)\leq\frac{E\left[e^{sZ}\right]}{e^{st}},\ \forall s>0\ \text{by Markov's inequality.}
$$

Chernoff's bound is based on finding the value of s that minimizes the upper bound. If Z is a sum of independent random variables. For example, say
Equation:

$$
Z=\sum_{i=1}^{n}(\ell\left(f\left(X_i\right),Y_i\right)-R\left(f\right))=n\left(\widehat{R}_n\left(f\right)-R\left(f\right)\right)
$$

then the bound becomes
Equation:

$$P\left(\sum_{i=1}^{n}\left(L_i - E\left[L_i\right]\right) \geq t\right) \leq e^{-st} E\left[e^{s\sum_{i=1}^{n}(L_i - E[L_i])}\right] \leq e^{-st}\prod_{i=1}^{n} E\left[e^{s(L_i - E[L_i])}\right], \text{ from independence.}$$

Thus, the problem of finding a tight bound boils down to finding a good bound for $E\left[s^{s(L_i - E[L_i])}\right]$. Chernoff ('52), first studied this situation for binary random variables. Then, Hoeffding ('63) derived a more general result for arbitrary bounded random variables.

Hoeffding's Indequality

Theorem
Hoeffding's Inequality

Let $Z_1, Z_2, \ldots, Zn$ be independent bounded random variables such that $Z_i \in [a_i, b_i]$ with probability 1. Let $S_n = \sum_{i=1}^{n} Z_i$. Then for any $t > 0$, we have
Equation:

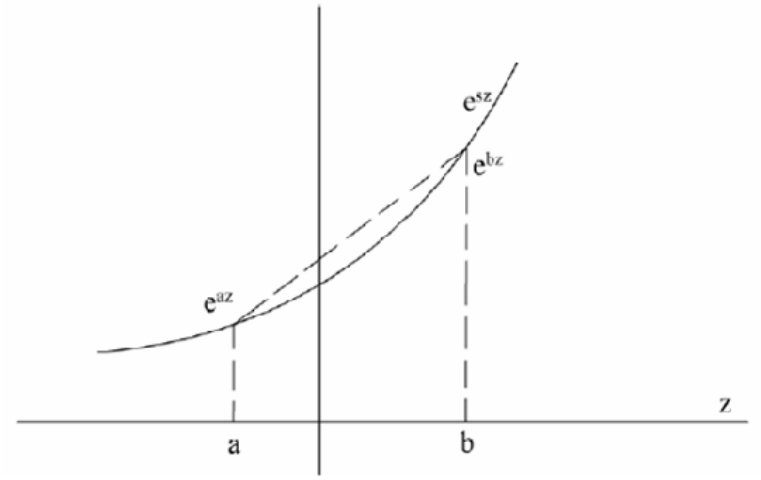
$$P(|S_n - E\left[S_n\right]| \geq t) \leq 2e^{-\frac{2t^2}{\sum_{i=1}^{n}(b_i - a_i)^2}}.$$

The key to proving Hoeffding's inequality is the following upper bound: if Z is a random variable with $E[Z] = 0$ and $a \leq Z \leq b$, then
Equation:

$$E\left[e^{sZ}\right] \leq e^{\frac{s^2(b-a)^2}{8}}.$$

This upper bound is derived as follows. By the convexity of the exponential function,
Equation:

$$e^{sz} \leq \frac{z-a}{b-a}e^{sb} + \frac{b-z}{b-a}e^{sa}, \text{ for } a \leq z \leq b.$$



Convexity of exponential function.

Thus,
Equation:

$$\begin{aligned} E\left[e^{sZ}\right] &\leq E\left[\frac{Z-a}{b-a}\right]e^{sb}+E\left[\frac{b-Z}{b-a}\right]e^{sa} \\ &= \frac{b}{b-a}e^{sa}-\frac{a}{b-a}e^{sb}\ ,\ \text{since } E[Z]=0 \\ &= \left(1-\theta+\theta e^{s(b-a)}\right)e^{-\theta s(b-a)}\ ,\ \text{where } \theta=\frac{-a}{b-a} \end{aligned}.$$

Now let
Equation:

$$u=s\left(b-a\right)\ \text{ and define }\ \varphi\left(u\right)\equiv -\theta u+\log\left(1-\theta+\theta e^{u}\right).$$

Then we have
Equation:

$$E\left[e^{sZ}\right]\leq\left(1-\theta+\theta e^{s(b-a)}\right)e^{-\theta s(b-a)}=e^{\varphi(u)}.$$

To minimize the upper bound let's express $\varphi(u)$ in a Taylor's series with remainder :
Equation:

$$\varphi\left(u\right)=\varphi\left(0\right)+u\varphi'\left(0\right)+\frac{u^{2}}{2}\varphi''\left(v\right)\ \text{ for some }\ v\in[0,u]$$

Equation:

$$\begin{aligned} \varphi'\left(u\right) &= -\theta+\frac{\theta e^{u}}{1-\theta+\theta e^{u}}\Rightarrow\varphi'\left(u\right)=0 \\ \varphi''\left(u\right) &= \frac{\theta e^{u}}{1-\theta+\theta e^{u}}-\frac{\left(\theta e^{u}\right)^{2}}{\left(1-\theta+\theta e^{u}\right)^{2}}\ . \\ &= \frac{\theta e^{u}}{1-\theta+\theta e^{u}}\left(1-\frac{\theta e^{u}}{1-\theta+\theta e^{u}}\right) \\ &= \rho(1-\rho) \end{aligned}$$

Now, $\varphi''\left(u\right)$ is maximized by
Equation:

$$\rho=\frac{\theta e^{u}}{1-\theta+\theta e^{u}}=\frac{1}{2}\Rightarrow\varphi''\left(u\right)\leq\frac{1}{4}.$$

So,
Equation:

$$\varphi(u) \leq \frac{u^2}{8} = \frac{s^2(b-a)^2}{8}$$

Equation:

$$\Rightarrow E\left[e^{sZ}\right] \leq e^{\frac{s^2(b-a)^2}{8}}.$$

Now, we can apply this upper bound to derive Hoeffding's inequality.
Equation:

$$\begin{aligned} P(S_n - E[S_n] \geq t) &\leq e^{-st}\prod_{i=1}^{n} E\left[e^{s(L_i - E[L_i])}\right] \\ &\leq e^{-st}\prod_{i=1}^{n} e^{\frac{s^2(b_i-a_i)^2}{8}} \\ &= e^{-st}e^{s^2\sum_{i=1}^{n}\frac{(b_i-a_i)^2}{8}} \\ &= e^{\frac{-2t^2}{\sum_{i=1}^{n}(b_i-a_i)^2}} \\ &\quad \text{by choosing} \quad s = \frac{4t}{\sum_{i=1}^{n}(b_i-a_i)^2} \end{aligned}$$

Similarly, $P(E[S_n] - S_n \geq t) \leq e^{\frac{-2t^2}{\sum_{i=1}^{n}(b_i-a_i)^2}}$. This completes the proof of the Hoeffding's theorem.

Example:
Application
Let $Z_i = 1_{f(X_i)\neq Y_i} - R(f)$, as in the classification problem. Then for a fixed f, it follows from Hoeffding's inequality (i.e., Chernoff's bound in this special case) that
Equation:

$$\begin{aligned} P\left(\left|\widehat{R_n}(f) - R(f)\right| \geq \epsilon\right) &= P\left(\frac{1}{n}|S_n - E[S_n]| \geq \epsilon\right) \\ &= P(|S_n - E[S_n]| \geq n\epsilon) \\ &\leq 2e^{-\frac{2(n\epsilon)^2}{n}} \\ &= 2e^{-2n\epsilon^2} \end{aligned}.$$

Now, we want a bound like this to hold uniformly for all $f \in \mathscr{F}$. Assume that $\mathscr{F}$ is a finite collection of models and let $|\mathscr{F}|$ denote its cardinality. We would like to bound the probability that
$\max_{f\in\mathscr{F}}\left|\widehat{R_n}(f) - R(f)\right| \geq \epsilon$. Note that the event
Equation:

$$\left\{\max_{f\in\mathscr{F}}\left|\widehat{R_n}(f) - R(f)\right| \geq \epsilon\right\} \equiv \left\{\bigcup_{f\in\mathscr{F}}\left|\widehat{R_n}(f) - R(f)\right| \geq \epsilon\right\}.$$

Therefore

Equation:

$$\begin{aligned} P\left(\max_{f\in\mathscr{F}}\left|\widehat{R_n}\left(f\right)-R\left(f\right)\right|\geq\epsilon\right) &= P\left(\bigcup_{f\in\mathscr{F}}\left|\widehat{R_n}\left(f\right)-R\left(f\right)\right|\geq\epsilon\right) \\ &\leq \sum_{f\in F}P(|\widehat{R_n}\left(f\right)-R\left(f\right)|\geq\epsilon),\ \text{the ``}union\ of\ events\text{''}\ \text{bound} \\ &\leq 2|F|e^{-2n\epsilon^2},\ \text{by Hoeffding's inequality.} \end{aligned}$$

Thus, we have shown that with probability at least $1-2|F|e^{-2n\epsilon^2}$, $\forall f\in\mathscr{F}$
Equation:

$$\left|\widehat{R_n}\left(f\right)-R\left(f\right)|<\epsilon.$$

And accordingly, we can be reasonably confident in selecting f from $\mathscr{F}$ based on the empirical risk function $\widehat{R}_n$.

Classification Error Bounds

Recap: Classifier design

Given a set of training data $\{X_i, Y_i\}_{i=1}^n$ and a finite collection of candidate functions $\mathscr{F}$, select $\widehat{f_n} \in \mathscr{F}$ that (hopefully) is a good predictor for future cases. That is
Equation:

$$\widehat{f_n} = \operatorname*{argmin}_{f \in \mathscr{F}} \widehat{R}_n(f)$$

where $\widehat{R}_n(f)$ is the empirical risk. For any particular $f \in \mathscr{F}$, the corresponding empirical risk is defined as
Equation:

$$\widehat{R}_n(f) = \frac{1}{n} \sum_{i=1}^{n} \mathbf{1}_{\{f(X_i) \neq Y_i\}}.$$

Hoeffding's inequality

Hoeffding's inequality (Chernoff's bound in this case) allows us to gauge how close $\widehat{R}_n(f)$ is to the true risk of f, $R(f)$, in probability
Equation:

$$P(|\widehat{R}_n(f) - R(f)| \geq \epsilon) \leq 2e^{-2n\epsilon^2}.$$

Since our selection process involves deciding among all $f \in \mathscr{F}$, we would like to gauge how close the empirical risks are to their expected values. We can do this by studying the probability that one or more of the empirical risks deviates significantly from its expected value. This is captured by the probability
Equation:

$$P\left(\max_{f \in \mathscr{F}} \left|\widehat{R}_n(f) - R(f)\right| \geq \epsilon\right).$$

Note that the event
Equation:

$$\max_{f \in \mathscr{F}} \left|\widehat{R}_n(f) - R(f)\right| \geq \epsilon$$

is equivalent to union of the events
Equation:

$$\bigcup_{f \in \mathscr{F}} \left\{\left|\widehat{R}_n(f) - R(f)\right| \geq \epsilon\right\}.$$

Therefore, we can use Bonferonni's bound (aka the “union of events” or “union” bound) to obtain
Equation:

$$\begin{aligned} P\left(\max_{f\in\mathscr{F}}\left|\widehat{R}_n\left(f\right)-R\left(f\right)\right|\geq\epsilon\right) &= P\left(\bigcup_{f\in\mathscr{F}}\left|\widehat{R}_n\left(f\right)-R\left(f\right)\right|\geq\epsilon\right) \\ &\leq \sum_{f\in\mathscr{F}}P(|\widehat{R}_n\left(f\right)-R\left(f\right)|\geq\epsilon) \\ &\leq \sum_{f\in\mathscr{F}}2e^{-2n\epsilon^2} \\ &= 2|\mathscr{F}|e^{-2n\epsilon^2} \end{aligned}$$

where $|\mathscr{F}|$ is the number of classifiers in $\mathscr{F}$. In the proof of Hoeffding's inequality we also obtained a one-sided inequality that implied
Equation:

$$P\left(R\left(f\right)-\widehat{R}_n\left(f\right)\geq\epsilon\right)\leq e^{-2n\epsilon^2}$$

and hence
Equation:

$$P\left(\max_{f\in\mathscr{F}}\ R\left(f\right)-\widehat{R}_n\left(f\right)\geq\epsilon\right)\leq|\mathscr{F}|e^{-2n\epsilon^2}.$$

We can restate the inequality above as follows, For all $f\in\mathscr{F}$ and for all $\delta>0$ with probability at least $1-\delta$
Equation:

$$R\left(f\right)\leq\widehat{R}_n\left(f\right)+\sqrt{\frac{\log|\mathscr{F}|+\log\left(1/\delta\right)}{2n}}.$$

This follows by setting $\delta=|\mathscr{F}|e^{-2n\epsilon^2}$ and solving for ϵ. Thus with a high probability $(1-\delta)$, the true risk for all $f\in\mathscr{F}$ is bounded by the empirical risk of f plus a constant that depends on $\delta>0$, the number of training samples n, and the size $\mathscr{F}$. Most importantly the bound does not depend on the unknown distribution P_{XY}. Therefore, we can call this a **distribution-free** bound.

Error Bounds

We can use the **distribution-free** bound above to obtain a bound on the expected performance of the minimum empirical risk classifier
Equation:

$$\widehat{f}_n=\operatorname*{argmin}_{f\in\mathscr{F}}\widehat{R}_n\left(f\right).$$

We are interested in bounding

Equation:

$$E\left[R\left(\widehat{f}_n\right)\right]-\min_{f\in\mathscr{F}}R\left(f\right)$$

the expected risk of $\widehat{f}_n$ minus the minimum risk for all $f\in\mathscr{F}$. Note that this difference is always non-negative since $\widehat{f}_n$ is at best as good as
Equation:

$$f^*=\operatorname*{argmin}_{f\in\mathscr{F}}R\left(f\right).$$

Recall that $\forall f\in\mathscr{F}$ and $\forall\delta>0$, with probability at least $1-\delta$
Equation:

$$R\left(f\right)\leq\widehat{R}_n\left(f\right)+C\left(\mathscr{F},n,\delta\right)$$

where
Equation:

$$C\left(\mathscr{F},n,\delta\right)=\sqrt{\frac{\log\left|\mathscr{F}\right|+\log\left(1/\delta\right)}{2n}}.$$

In particular, since this holds for all $f\in\mathscr{F}$ including $\widehat{f}_n$,
Equation:

$$R\left(\widehat{f}_n\right)\leq\widehat{R}_n\left(\widehat{f}_n\right)+C\left(\mathscr{F},n,\delta\right)$$

and for any other $f\in\mathscr{F}$
Equation:

$$R\left(\widehat{f}_n\right)\leq\widehat{R}_n\left(f\right)+C\left(\mathscr{F},n,\delta\right)$$

since $\widehat{R}_n\left(\widehat{f}_n\right)\leq\widehat{R}_n\left(f\right)\forall f\in\mathscr{F}$. In particular,
Equation:

$$R\left(\widehat{f}_n\right)\leq\widehat{R}_n\left(f^*\right)+C\left(\mathscr{F},n,\delta\right)$$

where $f^*=\operatorname{argmin}_{f\in\mathscr{F}}R\left(f\right)$.

Let Ω denote the set of events on which the above inequality holds. Then by definition
Equation:

$$P(\Omega)\geq1-\delta.$$

We can now bound $E\left[R\left(\widehat{f}_n\right)\right]-R\left(f^*\right)$ as follows

Equation:

$$\begin{aligned} E\left[R\left(\widehat{f}_n\right)\right]-R\left(f^*\right) &= E\Big[R\left(\widehat{f}_n\right)-\widehat{R}_n\left(f^*\right)+\widehat{R}_n\left(f^*\right)-R\left(f^*\right)\Big] \\ &= E\Big[R\left(\widehat{f}_n\right)-\widehat{R}_n\left(f^*\right)\Big] \end{aligned}$$

since $E\left[\widehat{R}_n\left(f^*\right)\right]=R\left(f^*\right)$. The quantity above is bounded as follows.

Equation:

$$\begin{aligned} E\Big[R\left(\widehat{f}_n\right)-\widehat{R}_n\left(f^*\right)\Big] &= E\left[R\left(\widehat{f}_n\right)-\widehat{R}_n\left(f^*\right)\Big|\Omega\right]P\left(\Omega\right)+E\left[R\left(\widehat{f}_n\right)-\widehat{R}_n\left(f^*\right)\Big|\Omega\right]P\left(\overline{\Omega}\right) \\ &\leq E\Big[R\left(\widehat{f}_n\right)-\widehat{R}_n\left(f^*\right)\Big|\Omega\Big]+\delta \end{aligned}$$

since $P(\Omega)\leq 1$, $1-P(\Omega)\leq\delta$ and $R\left(\widehat{f}_n\right)-\widehat{R}_n\left(f^*\right)\leq 1$

Equation:

$$\begin{aligned} E\Big[R\left(\widehat{f}_n\right)-\widehat{R}_n\left(f^*\right)\Big|\Omega\Big] &\leq E\Big[R\left(\widehat{f}_n\right)-\widehat{R}_n\left(\widehat{f}_n\right)\Big|\Omega\Big]. \\ &\leq C(\mathscr{F},n,\delta) \end{aligned}$$

Thus

Equation:

$$E\left[R\left(\widehat{f}_n\right)-\widehat{R}_n\left(f^*\right)\right]\leq C\left(\mathscr{F},n,\delta\right)+\delta.$$

So we have

Equation:

$$E\left[R\left(\widehat{f}_n\right)\right]-\min_{f\in\mathscr{F}}R\left(f\right)\leq\sqrt{\frac{\log|\mathscr{F}|+\log\left(1/\delta\right)}{2n}}+\delta,\ \ \forall\delta>0.$$

In particular, for $\delta=\sqrt{1/n}$, we have

Equation:

$$\begin{aligned} E\left[R\left(\widehat{f}_n\right)\right]-\min_{f\in\mathscr{F}}R\left(f\right) &\leq \sqrt{\frac{\log|\mathscr{F}|+\log n}{2n}}+\frac{1}{\sqrt{n}} \\ &\leq \sqrt{\frac{\log|\mathscr{F}|+\log n+2}{n}}, \quad \text{since} \quad \sqrt{x}+\sqrt{y}\leq\sqrt{2}\sqrt{x+y},\ \forall\ x,y>0 \end{aligned}$$

.

Application: Histogram Classifier

Let $\mathscr{F}$ be the collection of all classifiers with M equal volume cells. Then $|\mathscr{F}| = 2^M$, and the histogram classification rule
Equation:

$$\widehat{f}_n = \operatorname{argmin}_{f \in \mathscr{F}} \left(\frac{1}{n} \sum_{i=1}^{n} 1_{\{f(X_i) \neq Y_i\}} \right)$$

satisfies
Equation:

$$E\left[R\left(\widehat{f}_n\right)\right] - \min_{f \in \mathscr{F}} R(f) \leq \sqrt{\frac{M \log 2 + 2 + \log n}{n}}$$

which suggests the choice $M = \log_2 n$ (balancing $M \log 2$ with $\log n$), resulting in
Equation:

$$E\left[R\left(\widehat{f}_n\right)\right] - \min_{f \in \mathscr{F}} R(f) = O\left(\sqrt{\frac{\log n}{n}}\right).$$

Error Bounds in Countably Infinite Spaces

Introduction

In the last lecture, we studied bounds of the following form: for any $\delta > 0$, with probability at least $1 - \delta$,
Equation:

$$R(f) \leq \widehat{R}_n(f) + \sqrt{\frac{\log|\mathscr{F}| + \log\left(\frac{1}{\delta}\right)}{2n}} \quad , \quad \forall f \in \mathscr{F}$$

which led to upper bounds on the estimation error of the form
Equation:

$$E\left[R\left(\widehat{f}_n\right)\right] - \min_{f \in F} R(f) \;\leq\; \sqrt{\frac{\log|\mathscr{F}| + \log(n) + 2}{n}}.$$

The key assumptions made in deriving the error bounds were:

- **(i)** bounded loss function
- **(ii)** finite collection of candidate functions

The bounds are valid for every P_{XY} and are called distribution-free .

Deriving Bounds for Countably Infinite Spaces

In this lecture we will generalize the previous results in a powerful way by developing bounds applicable to possibly infinite collections of candidates. To start let us suppose that $\mathscr{F}$ is a countable, possibly infinite, collection of candidate functions. Assign a positive number c(f) to each $f \in \mathscr{F}$, such that
Equation:

$$\sum_{f \in \mathscr{F}} e^{-c(f)} < \infty.$$

The numbers c(f) can be interpreted as

- **(i)** measures of complexity
- **(ii)** -log of prior probabilities
- **(iii)** codelengths

In particular, if P(f) is the prior probability of f then
Equation:

$$e^{-(-\log p(f))} = p(f)$$

so $c(f) \equiv -\log p(f)$ produces
Equation:

$$\sum_{f \in \mathscr{F}} e^{-c(f)} = \sum_{f \in \mathscr{F}} p\left(f\right) = 1.$$

Now recall Hoeffding's inequality. For each f and every $\epsilon > 0$
Equation:

$$P\Big(R\left(f\right) - \widehat{R}_n\left(f\right) \geq \epsilon\Big) \leq e^{-2n\epsilon^2}$$

or for every $\delta > 0$
Equation:

$$P\left(R\left(f\right) - \widehat{R}_n\left(f\right) \geq \sqrt{\frac{\log\left(\frac{1}{\delta}\right)}{2n}}\right) \leq \delta.$$

Suppose $\delta > 0$ is specified. Using the values c(f) for $f \in \mathscr{F}$, define
Equation:

$$\delta\left(f\right) = e^{-c(f)}\delta.$$

Then we have
Equation:

$$P\left(R\left(f\right) - \widehat{R}_n\left(f\right) \geq \sqrt{\frac{\log\left(\frac{1}{\delta(f)}\right)}{2n}}\right) \leq \delta\left(f\right).$$

Furthermore we can apply the union bound as follows
Equation:

$$\begin{aligned} P\left(\sup_{f \in \mathscr{F}}\left\{R\left(f\right) - \widehat{R}_n\left(f\right) - \sqrt{\frac{\log\left(1/\delta(f)\right)}{2n}}\right\} \geq 0\right) &\leq P\left(\bigcup_{f \in \mathscr{F}} R\left(f\right) - \widehat{R}_n\left(f\right) \geq \sqrt{\frac{\log\left(\frac{1}{\delta(f)}\right)}{2n}}\right) \\ &\leq \sum_{f \in \mathscr{F}} P\left(R\left(f\right) - \widehat{R}_n\left(f\right) \geq \sqrt{\frac{\log\left(\frac{1}{\delta(f)}\right)}{2n}}\right). \\ &\leq \sum_{f \in \mathscr{F}} \delta\left(f\right) = \sum_{f \in \mathscr{F}} e^{-c(f)}\delta = \delta \end{aligned}$$

So for any $\delta > 0$ with probability at least $1 - \delta$, we have that $\forall f \in \mathscr{F}$
Equation:

$$\begin{aligned} R(f) &\leq \widehat{R}_n(f) + \sqrt{\frac{\log\left(\frac{1}{\delta(f)}\right)}{2n}} \\ &= \widehat{R}_n(f) + \sqrt{\frac{c(f) + \log\left(\frac{1}{\delta}\right)}{2n}} \end{aligned}.$$

Special Case
Suppose $\mathscr{F}$ is finite and $c(f) = \log|\mathscr{F}| \quad \forall f \in \mathscr{F}$. Then
Equation:

$$\sum_{f\in\mathscr{F}} e^{-c(f)} = \sum_{f\in\mathscr{F}} e^{-\log|\mathscr{F}|} = \sum_{f\in\mathscr{F}} \frac{1}{|\mathscr{F}|} = 1$$

and
Equation:

$$\delta(f) = \frac{\delta}{|\mathscr{F}|}$$

which implies that for any $\delta > 0$ with probability at least $1-\delta$, we have
Equation:

$$R(f) \leq \widehat{R}_n(f) + \sqrt{\frac{\log|\mathscr{F}| + \log\left(\frac{1}{\delta(f)}\right)}{2n}} \quad , \qquad \forall f \in \mathscr{F}.$$

Note that this is precisely the bound we derived in the last lecture.

Choosing c(f)

The generalized bounds allow us to handle countably infinite collections of candidate functions, but we require that
Equation:

$$\sum_{f\in\mathscr{F}} e^{-c(f)} < \infty.$$

Of course, if $c(f) = -\log p(f)$ where $p(f)$ is a proper prior probability distribution then we have
Equation:

$$\sum_{f\in\mathscr{F}} e^{-c(f)} = 1.$$

However, it may be difficult to design a probability distribution over an infinite class of candidates. The coding perspective provides a very practical means to this end.

Assume that we have assigned a uniquely decodable binary code to each $f \in \mathscr{F}$, and let c(f) denote the codelength for f. That is, the code for f is c(f) bits long. A very useful class of uniquely decodable codes are called prefix codes .

Prefix Code

A code is called a prefix code if no codeword is a prefix of any other codeword.

Example:
From Cover & Thomas '91
Consider an alphabet of symbols, say A, B, C, and D and the codebooks below

Symbol	Singular Codebook	Nonsingular But Not Uniquely Decodable	Uniquely Decodable But Not a Prefix Code	Prefix Code
A	0	0	10	0
B	0	010	00	10
C	0	01	11	110
D	0	10	110	1110

In the singular codebook we assign the same codeword to each symbol - a system that is obviously flawed!
In the second case, the codes are not singular but the codeword 010 could represent B or CA or AD. Hence it is not a uniquely decodable codebook.
The third and fourth cases are both examples of uniquely decodable codebooks, but the fourth has the added feature that no codeword is a prefix of another. Prefix codes can be decoded from left to right since each codeword is “self-punctuating" - in this case with a zero to indicate the end of each word.
To design a uniquely decodable codebook in general is as challenging as the problem of selecting c(f) to satisfy
Equation:

$$\sum_{f \in \mathscr{F}} e^{-c(f)} < \infty.$$

However, prefix codes can often be easily designed or specified and they are inherently decodable. Moreover, prefix codes satisfy an important inequality called the Kraft Inequality .

The Kraft Inequality

For any binary prefix code, the codeword lengths c_1, c_2, ... satisfy
Equation:

$$\sum_{i=1}^{\infty} 2^{-c_i} \leq 1.$$

Conversely, given any c_1, c_2, ... satisfying the inequality above we can construct a prefix code with these codeword lengths. We will prove this result a bit later, but now let's see how this is useful in our learning problem.

Assume that we have assigned a binary prefix codeword to each $f \in \mathscr{F}$, and let c(f) denote the bit-length of the codeword for f. Set $\delta\,(f) = 2^{-c(f)}\delta$. Then
Equation:

$$P\left(\bigcup_{f\in\mathscr{F}} R\left(f\right)-\widehat{R}_n\left(f\right)\geq\sqrt{\frac{\log\left(\frac{1}{\delta(f)}\right)}{2n}}\right) \leq \sum_{f\in\mathscr{F}} P\left(R\left(f\right)-\widehat{R}_n\left(f\right)\geq\sqrt{\frac{\log\left(\frac{1}{\delta(f)}\right)}{2n}}\right).$$
$$\leq \sum_{f\in\mathscr{F}}\delta\left(f\right)=\sum_{f\in\mathscr{F}}2^{-c(f)}\delta=\delta$$

This implies that for any $\delta>0$ with probability at least $1-\delta$ we have $\forall f\in\mathscr{F}$
Equation:

$$R(f) \leq \widehat{R}_n\left(f\right)+\sqrt{\frac{\log\left(\frac{1}{\delta(f)}\right)}{2n}}$$
$$= \widehat{R}_n\left(f\right)+\sqrt{\frac{c\left(f\right)\log 2+\log\left(\frac{1}{\delta}\right)}{2n}}.$$

Application
Let $\mathscr{F}_1$, $\mathscr{F}_1$, ... be a sequence of finite sets of candidate functions with $|\mathscr{F}_1|<|\mathscr{F}_1|<\ldots$ We can design prefix codes as follows. Use the codes 0, 10, 110, 1110, ... to encode the subscript i in $|\mathscr{F}_i|$. For each class $|\mathscr{F}_i|$, construct a set of binary codewords of length $\lceil\log_2|\mathscr{F}|\rceil$ to uniquely encode each function in $\mathscr{F}_i$. Then, encode any given function f by first using the code for i corresponding to the smallest $\mathscr{F}_i$ that f belongs to, followed by the length $\lceil\log_2|\mathscr{F}|\rceil$ codeword for $f\in\mathscr{F}_i$. This is a prefix code.

Example:
Histogram Classifiers
X=[0,1]^d, Y={0,1}. Let $\mathscr{F}_k$, k=1, 2, ... denote the collection of histogram classification rules with k equal volume bins. We can use the following codebook for the index k.

k	Prefix Code
1	0
2	10
3	110
4	1110
.	.
.	.
.	.

And follow this codeword with $k=\log_2|\mathscr{F}_k|$ bits to indicate which of the 2^k possible histogram rules is under consideration. Thus for any $f\in\mathscr{F}_k$ for some k ≥ 1 there is a prefix code of length
Equation:

$$c(f)=k+k=2k \quad bits.$$

It follows that for any $\delta>0$ with probability at least $1-\delta$ we have $\forall f\in\bigcup_{k\geq1}\mathscr{F}_k$
Equation:

$$R\left(f\right)\leq\widehat{R}_n\left(f\right)+\sqrt{\frac{2k_f\log 2+\log\left(\frac{1}{\delta}\right)}{2n}}$$

where k_f is the number of bins in histogram corresponding to f. Contrast with the bound we had for the class of m bin histograms alone: with probability $\geq 1-\delta$, $\forall f\in\mathscr{F}_m$

Equation:

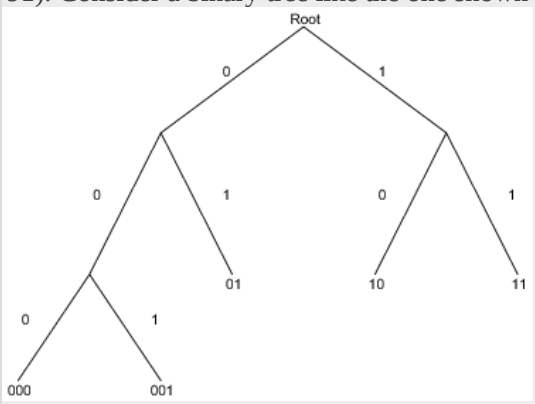
$$R(f) \leq \widehat{R}_n(f) + \sqrt{\frac{m \log 2 + \log\left(\frac{1}{\delta(f)}\right)}{2n}}.$$

Notice the bound for all histograms rules is almost as good as the bound for only the m-bin rules. That is, when $k_f = m$ the bounds are within a factor of $\sqrt{2}$. On the other hand, the new bound is a big improvement, since it also gives us a guide for selecting the number of bins.

Proof

Proof of the Kraft Inequality

We will prove that for any binary prefix code, the codeword lengths c_1, c_2, ... satisfy $\sum_{k \geq 1} 2^{-c_k} \leq 1$. The converse is easy to prove also, but it not central to our purposes here (for a proof, see Cover & Thomas '91). Consider a binary tree like the one shown below.



The sequence of bit values leading from the root to a leaf of the tree represents a codeword. The prefix condition implies that no codeword is a descendant of any other codeword in the tree. Let c_{max} be the length of the longest codeword (also the number of branches to the deepest leaf) in the tree.

Consider a leaf i in the tree at level c_i. This leaf would have $2^{c_{max}-c_i}$ descendants at level c_{max}. Furthermore, for each leaf the set of possible descendants at level c_{max} is disjoint (since no codeword can be a prefix of another). Therefore, since the total number of possible leafs at level c_{max} is $2^{c_{max}}$, we have

Equation:

$$\sum_{i \in \text{leafs}} 2^{c_{max}-c_i} \leq 2^{c_{max}} \quad \Rightarrow \quad \sum_{i \in \text{leafs}} 2^{-c_i} \leq 1$$

which proves the case when the number of codewords is finite.

Suppose now that we have a countably infinite number of codewords. Let $\mathrm{b}_1\ \mathrm{b}_2$ ... b_{c_i} be the ith codeword and let

Equation:

$$r_i = \sum_{j=i}^{c_i} b_j 2^{-j}$$

be the real number corresponding to the binary expansion of the codeword. We can associate the interval $[r_i, r_i + 2^{-c_i})$ with the ith codeword. This is the set of all real numbers whose binary expansion begins with $\mathrm{b}_1\ \mathrm{b}_2$ ... b_{c_i}. Since this is a subinterval of $[0, 1]$, and all such subintervals corresponding to prefix codewords are disjoint, the sum of their lengths must be less than or equal to 1. This proves the case where the number of codewords is infinite.

Complexity Regularization

Review: PAC Bounds

Consider a finite collection of models $\mathscr{F}$, and recall the basic PAC bound: for any $\delta > 0$, with probability at least $1 - \delta$
Equation:

$$R\left(f\right) \leq \widehat{R}_n\left(f\right) + \sqrt{\frac{\log\left|\mathscr{F}\right| + \log\left(1/\delta\right)}{2n}} \quad , \qquad \forall f \in \mathscr{F}$$

where
Equation:

$$\begin{aligned} \widehat{R}_n\left(f\right) &= \frac{1}{n}\sum_{i=1}^{n} \ell\left(f\left(X_i\right), Y_i\right) \\ R(f) &= E[\ell(f(X), Y)] \end{aligned}$$

and the loss ℓ is assumed to be bounded between 0 and 1. Note that we can write the inequality above as:
Equation:

$$R\left(f\right) \leq \widehat{R}_n\left(f\right) + \sqrt{\frac{\log\left(\frac{\left|\mathscr{F}\right|}{\delta}\right)}{2n}}$$

Letting $\delta_f = \frac{\delta}{\left|\mathscr{F}\right|}$, we have:
Equation:

$$R\left(f\right) \leq \widehat{R}_n\left(f\right) + \sqrt{\frac{\log\left(1/\delta_f\right)}{2n}}$$

This is precisely the form of Hoeffding's inequality, with δ_f in place of the usual δ. In effect, in order to have Hoeffding's inequality hold with probability $1 - \delta$ for all $f \in \mathscr{F}$, we must distribute the "δ-budget" or "confidence-budget" over all $f \in \mathscr{F}$ (in this case, evenly distributed):
Equation:

$$\begin{aligned} \sum_{f \in \mathscr{F}} \delta_f &= \sum_{f \in \mathscr{F}} \frac{\delta}{\left|\mathscr{F}\right|} \\ &= \delta \end{aligned}$$

However, to apply the union bound, we do not need to distribute δ evenly among the candidate models. We only require:
Equation:

$$\sum_{f \in \mathscr{F}} \delta_f \;\; = \;\; \delta$$

So, if $p(f)$ are positive numbers satisfying $\sum_{f \in \mathscr{F}} p\left(f\right) = 1$, then we can take $\delta_f = p\left(f\right)\delta$. This provides two advantages:

1. By choosing $p(f)$ larger for certain f, we can preferentially treat those candidates
2. We do not need $\mathscr{F}$ to be finite and we only require $\sum_{f \in \mathscr{F}} p\left(f\right) = 1$

Prefix codes are one way to achieve this. If we assign a binary prefix code of length $c(f)$ to each $f \in \mathscr{F}$, then the values $p\left(f\right) = 2^{-c(f)}$ satisfy $\sum_{f \in \mathscr{F}} p\left(f\right) \leq 1$ according to the Kraft inequality.

The main point of this lecture is to examine how PAC bounds of the form w.p. $\geq 1 - \delta$
Equation:

$$R\left(f\right) \leq \widehat{R}_n\left(f\right) + \sqrt{\frac{c(f)\,\log 2 + \log\left(1/\delta\right)}{2n}} \quad , \qquad \forall f \in \mathscr{F}$$

can be used to select a model that comes close to achieving the best possible performace
Equation:

$$\inf_{f \in \mathscr{F}} R\left(f\right)$$

Let $\widehat{f}_n$ be the model selected from $\mathscr{F}$ using the training data $\left\{X_i, Y_i\right\}_{i=1}^n$. We will specify this model in a moment, but keep in mind that it is not necessarily the model with minimum empirical risk as before. We would like to have
Equation:

$$E\left[R\left(\widehat{f}_n\right)\right] - \inf_{f \in \mathscr{F}} R\left(f\right)$$

as small as possible. First, for any $\delta > 0$, define
Equation:

$$\widehat{f}_n^{\delta} \;\; = \;\; \operatorname*{argmin}_{f \in \mathscr{F}} \left\{\widehat{R}_n\left(f\right) + C\left(f, n, \delta\right)\right\}$$

where
Equation:

$$C\left(f, n, \delta\right) \equiv \sqrt{\frac{c(f)\,\log 2 + \log\left(1/\delta\right)}{2n}}$$

Then w.p. $\geq 1 - \delta$
Equation:

$$R(f) \leq \widehat{R}_n(f) + C(f,n,\delta) \quad , \qquad \forall f \in \mathscr{F}$$

and in particular,
Equation:

$$R\left(\widehat{f}_n^{\delta}\right) \leq \widehat{R}_n\left(\widehat{f}_n^{\delta}\right) + C\left(\widehat{f}_n^{\delta}, n, \delta\right) \ ,$$

so, by the definition of $\widehat{f}_n^{\delta}$, $\forall f \in \mathscr{F}$
Equation:

$$R\left(\widehat{f}_n^{\delta}\right) \leq \widehat{R}_n(f) + C(f,n,\delta) \ .$$

We will make use of the inequality above in a moment. First note that $\forall f \ \in \mathscr{F}$
Equation:

$$E\left[R\left(\widehat{f}_n^{\delta}\right)\right] - R(f) \ = \ E\left[R\left(\widehat{f}_n^{\delta}\right) - \widehat{R}_n(f)\right] + E\left[\widehat{R}_n(f) - R(f)\right]$$

The second term is exactly 0, since $E\Big[\widehat{R}_n(f)\Big] = R(f)$.

Now consider the first term $E\Big[R\left(\widehat{f}_n^{\delta}\right) - \widehat{R}_n(f)\Big]$. Let Ω be the set of events on which
Equation:

$$R\left(\widehat{f}_n^{\delta}\right) \leq \widehat{R}_n(f) - C(f,n,\delta), \ \forall \ f \in \mathscr{F}$$

From the bound above, we know that $P(\Omega) \geq 1-\delta$. Thus,
Equation:

$$\begin{aligned} E\Big[R\left(\widehat{f}_n^{\delta}\right) - \widehat{R}_n(f)\Big] \ &= \ E\left[R\left(\widehat{f}_n^{\delta}\right) - \widehat{R}_n(f)\Big|\Omega\right]P(\Omega) + E\left[R\left(\widehat{f}_n^{\delta}\right) - \widehat{R}_n(f)\Big|\Omega^c\right](1-P(\Omega)) \\ &\leq \ C(f,n,\delta) + \delta \quad \Big(\text{since } 0 \leq R, \ \widehat{R} \leq 1, \ P(\Omega) \leq 1 \text{ and } 1-P(\Omega) \leq \delta\Big) \\ &= \ \sqrt{\frac{c(f)\,\log 2 + \log(1/\delta)}{2n}} + \delta \\ &= \ \sqrt{\frac{c(f)\,\log 2 + \frac{1}{2}\log n}{2n}} + \frac{1}{\sqrt{n}} \quad \left(\text{by} \quad \text{setting } \delta = \frac{1}{\sqrt{n}}\right) \end{aligned}$$

We can summarize our analysis with the following theorem.
Theorem
Complexity Regularized Model Selection

Let $\mathscr{F}$ be a countable collection of models, and assign a positive number $c(f)$ to each $f \in \mathscr{F}$ such that $\sum_{f \in \mathscr{F}} 2^{-c(f)} \leq 1$. Define the minimum complexity regularized risk model
Equation:

$$\widehat{f}_n \;\; = \;\; \underset{f \in \mathscr{F}}{\operatorname{argmin}} \left\{ \widehat{R}_n(f) + \sqrt{\frac{c(f) \log 2 + \frac{1}{2} \log n}{2n}} \right\}$$

Then,
Equation:

$$E\left[R\left(\widehat{f}_n\right)\right] \;\leq \inf_{f \in \mathscr{F}} \left\{ R(f) + \sqrt{\frac{c(f) \log 2 + \frac{1}{2} \log n}{2n}} + \frac{1}{\sqrt{n}} \right\}$$

This shows that
Equation:

$$\widehat{R}_n(f) + \sqrt{\frac{c(f) \log 2 + \frac{1}{2} \log n}{2n}}$$

is a reasonable surrogate for
Equation:

$$R(f) + \sqrt{\frac{c(f) \log 2 + \frac{1}{2} \log n}{2n}}$$

Example:
Histogram Classifiers
Let $\mathscr{X} = [0,1]^d$ be the input space and $\mathscr{Y} = \{0,1\}$ be the output space. Let $\mathscr{F}_k$, k = 1, 2, ... denotes the collection of histogram classification rules with k equal volume bins. One choice of prefix code for this example is: $k = 1 \Rightarrow \text{code} = 0, k = 3 \Rightarrow \text{code} = 10, k = 3 \Rightarrow \text{code} = 110$ and so on .... Then, if first code is corresponding to k $\Rightarrow f \in \mathscr{F}_k$, followed by $k = \log_2 |\mathscr{F}_k|$ bits to indicate which of the 2^k histogram rules in $\mathscr{F}_k$ is under consideration, we have
Equation:

$$f \in \mathscr{F}_k \Rightarrow c(f) = 2k \; bits$$

Let $\widehat{f}_n$ be the model that solves the minimization **i.e.,**
Equation:

$$\min_{k \geq 1} \left\{ \min_{f \in \mathscr{F}_k} \widehat{R}_n(f) + \sqrt{\frac{2k \log 2 + \frac{1}{2} \log n}{2n}} \right\}$$

That is, for each k, let

Equation:

$$\widehat{f}_n^{(k)} = \operatorname{argmin}_{f \in \mathscr{F}_k} \widehat{R}_n(f)$$

Then select the best k according to

Equation:

$$\widehat{k} = \operatorname{argmin}_{k \geq 1} \left\{ \widehat{R}_n\left(\widehat{f}_n^{(k)}\right) + \sqrt{\frac{2k \log 2 + \frac{1}{2} \log n}{2n}} \right\}$$

and set

Equation:

$$\widehat{f}_n = \widehat{f}_n^{\left(\widehat{k}\right)}$$

Then,

Equation:

$$E\left[R\left(\widehat{f}_n\right)\right] \leq \inf_{k \geq 1} \left\{ \min_{f \in \mathscr{F}_k} R(f) + \sqrt{\frac{2k \log 2 + \frac{1}{2} \log n}{2n}} + \frac{1}{\sqrt{n}} \right\}$$

It is a simple exercise to show that if $d = 2$ and the Bayes decision boundary is a 1-d curve, then by setting $k = \sqrt{n}$ and selecting the best f from $\mathscr{F}_{\sqrt{n}}$ we have

Equation:

$$E\left[R\left(\widehat{f}_n\right)\right] = O\left(n^{-1/4}\right)$$

Note: The complexity regularized classifier $\widehat{f}_n$ adaptively achieves this rate, without user intervention.

Decision Trees

Minimum Complexity Penalized Function

Recall the basic results of the last lectures: let $\mathscr{X}$ and $\mathscr{Y}$ denote the input and output spaces respectively. Let $X \in \mathscr{X}$ and $Y \in \mathscr{X}$ be random variables with unknown joint probability distribution P_{XY}. We would like to use X to "predict" Y. Consider a loss function $0 \leq \ell(y_1, y_2) \leq 1, \ \forall y_1, y_2 \in \mathscr{Y}$. This function is used to measure the accuracy of our prediction. Let $\mathscr{F}$ be a collection of candidate functions (models), $f : \mathscr{X} \to \mathscr{Y}$. The expected risk we incur is given by $R(f) \equiv E_{XY}[\ell(f(X), Y)]$. We have access only to a number of i.i.d. samples, $\{X_i, Y_i\}_{i=1}^n$. These allow us to compute the empirical risk $\widehat{R}_n(f) \equiv \frac{1}{n} \sum_{i=1}^n \ell(f(X_i), Y_i)$.

Assume in the following that $\mathscr{F}$ is countable. Assign a positive number $c(f)$ to each $f \in \mathscr{F}$ such that $\sum_{f \in \mathscr{F}} 2^{-c(f)} \leq 1$. If we use a prefix code to describe each element of $\mathscr{F}$ and define $c(f)$ to be the codeword length (in bits) for each $f \in \mathscr{F}$, the last inequality is automatically satisfied.

We define the **minimum complexity penalized estimator** as
Equation:

$$\widehat{f}_n \equiv \underset{f \in \mathscr{F}}{\operatorname{argmin}} \left\{ \widehat{R}_n(f) + \sqrt{\frac{c(f) \log 2 + \frac{1}{2} \log n}{2n}} \right\}.$$

As we showed previously we have the bound
Equation:

$$E\left[R\left(\widehat{f}_n\right)\right] \leq \min_{f \in \mathscr{F}} \left\{ R(f) + \sqrt{\frac{c(f) \log 2 + \frac{1}{2} \log n}{2n}} + \frac{1}{\sqrt{n}} \right\}.$$

The performance (risk) of $\widehat{f}_n$ is on average better than
Equation:

$$R\left(f_n^*\right) + \sqrt{\frac{c\left(f_n^*\right) \log 2 + \frac{1}{2} \log n}{2n}} + \frac{1}{\sqrt{n}},$$

where
Equation:

$$f_n^* = \operatorname{argmin}_{f \in \mathscr{F}} \left\{ R(f) + \sqrt{\frac{c(f) \log 2 + \frac{1}{2} \log n}{2n}} \right\}.$$

If it happens that the optimal function, that is
Equation:

$$f^* = \arg \min_{f \text{ measurable}} R(f),$$

is close to an $f \in \mathscr{F}$ with a small $c(f)$, then $\widehat{f}_n$ will perform almost as well as the optimal function.

Example:
Suppose $f^* \in \mathscr{F}$, then
Equation:

$$E\left[R\left(\widehat{f}_n\right)\right] \leq R\left(f^*\right) + \sqrt{\frac{c\left(f^*\right) \log 2 + \frac{1}{2} \log n}{2n}} + \frac{1}{\sqrt{n}}.$$

Furthermore if $c\left(f^*\right) = O(\log n)$ then
Equation:

$$E\left[R\left(\widehat{f}_n\right)\right] \leq R\left(f^*\right) + O\left(\sqrt{\frac{\log n}{n}}\right),$$

that is, only within a small $O\left(\sqrt{\frac{\log n}{n}}\right)$ offset of the optimal risk.

In general, we can also bound the excess risk $E\left[R\left(\widehat{f}_n\right)\right] - R^*$, where R^* is the Bayes risk,
Equation:

$$R^* = \inf_{f \text{ measurable}} R(f).$$

By subtracting R^* (a constant) from both sides of the inequality
Equation:

$$E\left[R\left(\widehat{f}_n\right)\right] \leq \min_{f \in \mathscr{F}} \left\{ R(f) + \sqrt{\frac{c(f)\log 2 + \frac{1}{2}\log n}{2n}} + \frac{1}{\sqrt{n}} \right\}$$

we obtain
Equation:

$$E\left[R\left(\widehat{f}_n\right)\right] - R^* \leq \min_{f \in \mathscr{F}} \left\{ R(f) - R^* + \sqrt{\frac{c(f)\log 2 + \frac{1}{2}\log n}{2n}} + \frac{1}{\sqrt{n}} \right\}.$$

Note that two terms in this upper bound: $R(f) - R^*$ is a bound on the approximation error of a model f, and remainder is a bound on the estimation error associated with f. Thus, we see that complexity regularization automatically optimizes a balance between approximation and estimation errors. In other words, complexity regularization is **adaptive** to the unknown tradeoff between approximation and estimation.

Classification

Consider the particularization of the above to a classification scenario. Let $\mathscr{X} = [0,1]^d$, $\mathscr{Y} = \{0,1\}$ and $\ell\left(\hat{y}, y\right) \equiv \mathbf{1}_{\{\hat{y} \neq y\}}$. Then $R(f) = E_{XY}\left[\mathbf{1}_{\{f(X) \neq Y\}}\right] = P\left(f(X) \neq Y\right)$. The Bayes risk is given by
Equation:

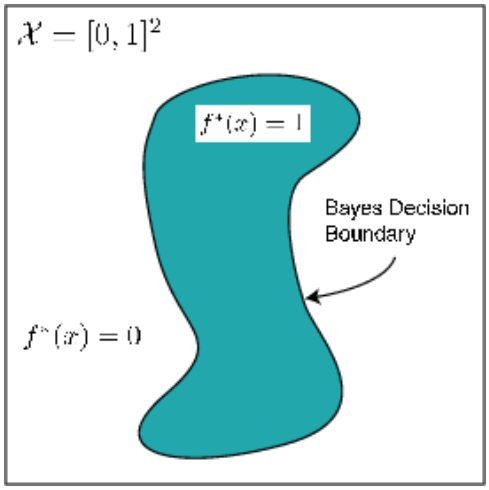
$$R^* = \inf_{f \text{ measurable}} R(f).$$

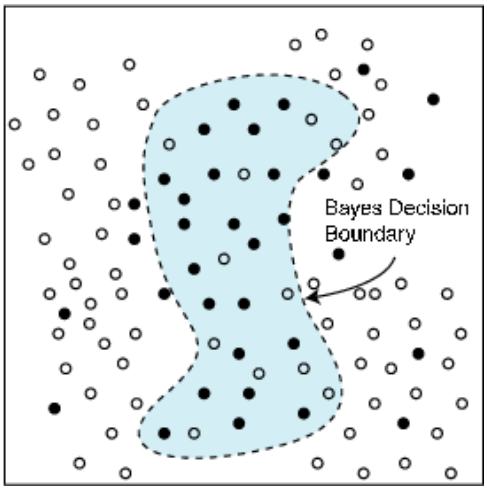
As it was observed before, the Bayes classifier (**i.e.,** a classifier that achieves the Bayes risk) is given by
Equation:

$$f^*(x) = \begin{cases} 1, & P(Y=1|X=x) \geq \frac{1}{2} \\ 0, & P(Y=1|X=x) < \frac{1}{2} \end{cases}.$$

This classifier can be expressed in a different way. Consider the set $G^* = \{x : \ P(Y=1|X=x) \geq 1/2\}$. The Bayes classifier can written as $f^*(x) = \mathbf{1}_{\{x \in G^*\}}$. Therefore the classifier is characterized entirely by the set G^*, if $X \in G^*$ then the "best" guess is that Y is one, and vice-versa. The boundary of this set corresponds to the points where the decision is harder. The boundary of G^* is called the **Bayes Decision Boundary**. In [link](a) this concept is illustrated. If $\eta(x) = P(Y=1|X=x)$ is a continuous function then the Bayes decision boundary is simply given by $\{x : \ P(Y=1|X=x) = 1/2\}$. Clearly the structure of the decision boundary provides important information on the difficulty of the problem.

(a) The Bayes classifier and the Bayes decision boundary ; (b) Example of the i.i.d. training pairs.





Empirical Classifier Design

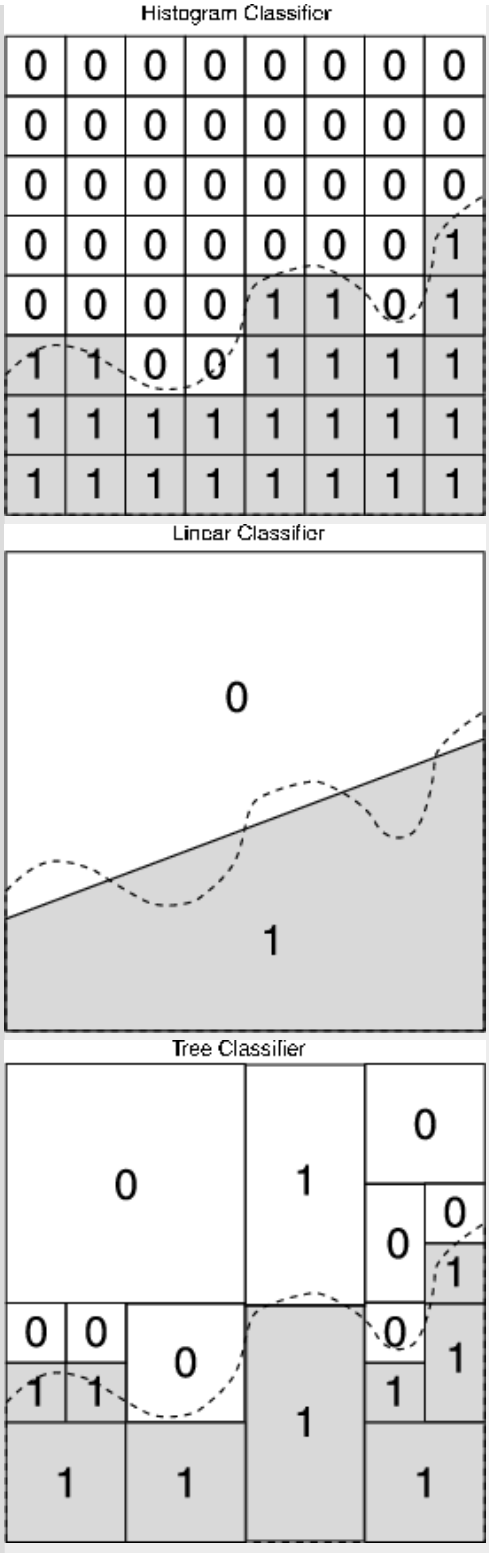
Given n i.i.d. training pairs, $\{X_i, Y_i\}_{i=1}^n$, we want to construct a classifier $\widehat{f}_n$ that performs well on average, **i.e.,** we want $E\left[R\left(\widehat{f}_n\right)\right]$ as close to R^* as possible. In [link](b) an example of the i.i.d. training pairs is depicted.

The construction of a classifier boils down to the estimation of the Bayes decision boundary. The histogram rule, discussed in a previous lecture, approaches the problem by subdividing the feature space into small boxes and taking a majority vote of the training data in each box. A typical result is depicted in [link](a).

The main problem with the histogram rule is that it is solving a more complicated problem than it is actually necessary. We do not need to determine the correct label for each individual box directly (the histogram rule is essentially estimating $\eta(x)$). In principle we only need to locate the decision boundary and assign the correct label on either side (notice that the accuracy of a majority vote over a region increases with the size of the region). The next example illustrates this.

Example:
Three Different Classifiers
The pictures below correspond to the approximation of the Bayes classifier by three different classifiers:

(a) Histogram classifier ; (b) Linear classifier; (c)Tree classifier.



The linear classifier and the tree classifier (to be defined formally later) both attack the problem of finding the boundary more directly than the histogram classifier, and therefore they tend to produce much better results in theory and practice. In the following we will demonstrate this for classification trees.

Binary Classification Trees

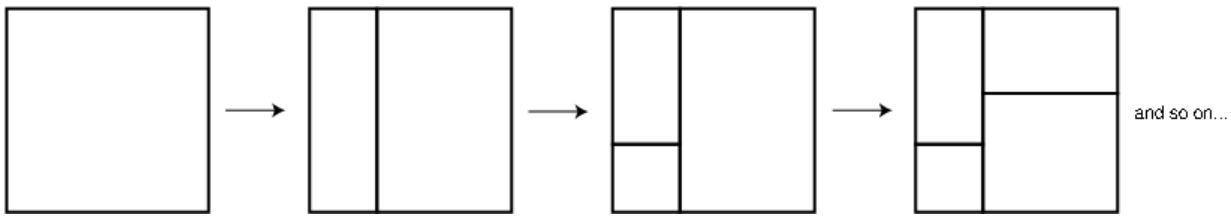
Binary classification trees are constructed by a two-step process:

1. Tree growing
2. Tree pruning

The basic idea is to first grow a very large, complicated tree classifier, that explains the the training data very accurately, but has poor generalization characteristics, and then prune this tree, to avoid overfitting.

Growing Trees

The growing process is based on recursively subudividing the feature space. Usually the subdivisions are splits of existing regions into two smaller regions (**i.e.,** binary splits) and usually the splits are perpendicular to one of the feature axes. An example of such construction is depicted in [link].

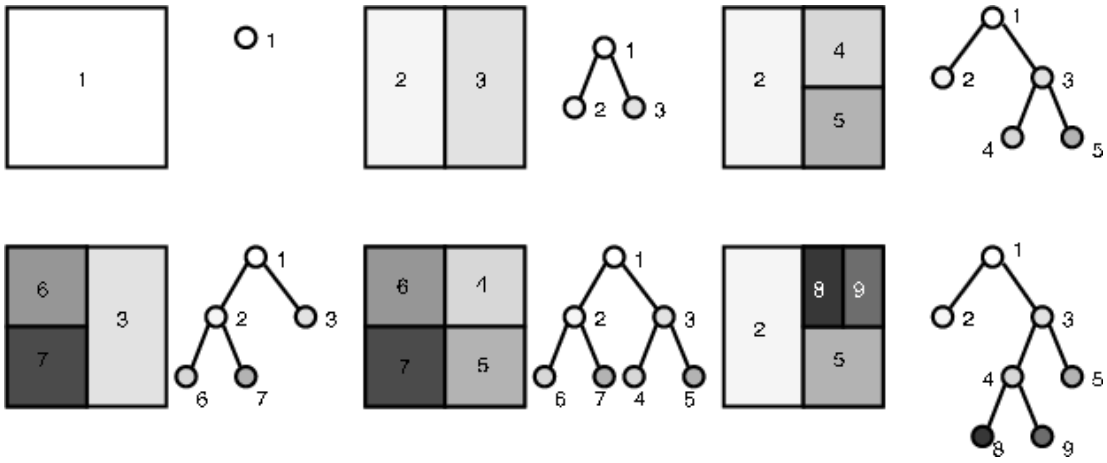


Growing a recursive binary tree ($\mathscr{X} = [0,1]^2$).

Often the splitting process is based on the training data, and is designed to separate data with different labels as much as possible. It such constructions, the “splits,” and hence the tree-structure itself, are data dependent. Alternatively, the splitting and subdivision could be independent from the training data. The latter approach is the one we are going to investigate in detail, and we will consider Dyadic Decision Trees and Recursive Dyadic Partitions (depicted in [link]) in particular.

Until now we have been referring to trees, but did not make clear how do trees relate to partitions. It turns out that any decision tree can be associated with a partition of the input space $\mathscr{X}$ and vice-versa. In particular, a Recursive Dyadic Partition (RDP) can be associated with a (binary) tree. In fact, this is the most efficient way of describing a

RDP. In [link] we illustrate the procedure. Each leaf of the tree corresponds to a cell of the partition. The nodes in the tree correspond to the various partition cells that are generated through in the construction of the tree. The orientation of the dyadic split alternates between the levels of the tree (for the example of [link], at the root level the split is done in the horizontal axis, at the level below that (the level of nodes 2 and 3) the split is done in the vertical axis, and so on...). The tree is called dyadic because the splits of cells are always at the midpoint along one coordinate axis, and consequently the sidelengths of all cells are dyadic (i.e., powers of 2).



Example of Recursive Dyadic Partition (RDP) growing ($\mathscr{X} = [0,1]^2$).

In the following we are going to consider the 2-dimensional case, but all the results can be easily generalized for the d-dimensional case ($d \geq 2$), provided the dyadic tree construction is defined properly. Consider a recursive dyadic partition of the feature space into k boxes of equal size. Associated with this partition is a tree T. Minimizing the empirical risk with respect to this partition produces the histogram classifier with k equal-sized bins. Consider also all the possible partitions corresponding to pruned versions of the tree T. Minimizing the empirical risk with respect to those other partitions results in other classifiers (dyadic decision trees) that are fundamentally different than the histogram rule we analyzed earlier.

Pruning

Let $\mathscr{F}$ be the collection of all possible dyadic decision trees corresponding to recursive dyadic partitions of the feature space. Each such tree can be prefix encoded

with a bit-string proportional to the number of leafs in the tree as follows; encode the structure of the tree in a top-down fashion: (i) assign a zero at each branch node and a one at each leaf node (terminal node) (ii) read the code in a breadth-first fashion, top-down, left-right. [link] exemplifies this coding strategy. Notice that, since we are considering binary trees, the total number of nodes is twice the number of leafs minus one, that is, if the number of leafs in the tree is k then the number of nodes is $2k-1$. Therefore to encode a tree with k leafs we need $2k-1$ bits.

Since we want to use the partition associated with this tree for classification we need to assign a decision label (either zero or one) to each leaf. Hence, to encode a decision tree in this fashion we need $3k-1$ bits, where k is the number of leafs. For a tree with k leafs the first $2k-1$ bits of the codeword encode the tree structure, and the remaining k bits encode the classification labels. This is easily shown to be a prefix code, therefore we can use this under our classification scenario.

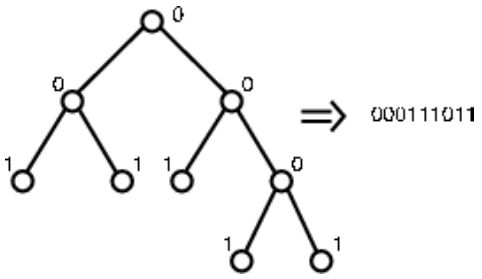


Illustration of the tree coding technique: example of a tree and corresponding prefix code.

Let
Equation:

$$\widehat{f}_n^* = \operatorname*{argmin}_{f \in \mathscr{F}} \left\{ \widehat{R}_n(f) + \sqrt{\frac{(3k-1)\log 2 + \frac{1}{2}\log n}{2n}} \right\}.$$

This optimization can be solved through a bottom-up pruning process (starting from a very large initial tree T_0) in $O(|T_0|^2)$ operations, where $|T_0|$ is the number of leafs in the initial tree. The complexity regularization theorem tells us that

Equation:

$$E\left[R\left(\widehat{f}_n\right)\right] \leq \min_{f \in \mathscr{F}} \left\{ R(f) + \sqrt{\frac{(3k-1)\log 2 + \frac{1}{2}\log n}{2n}} \right\} + \frac{1}{\sqrt{n}}.$$

Comparison between Histogram Classifiers and Classification Trees

In the following we will illustrate the idea behind complexity regularization by applying the basic theorem to histogram classifiers and classification trees (using our setup above).

Consider the classification setup described in "Classification", with $\mathscr{X} = [0,1]^2$.

Histogram Risk Bound

Recall the setup and results of a previous lecture[footnote]. Let
The description here is slightly different than the one in the previous lecture.
Equation:

$$\mathscr{F}_k^H = \{\text{histogram rules with } k^2 \text{ bins}\}.$$

Then $\left|\mathscr{F}_k^H\right| = 2^{k^2}$. Let $\mathscr{F}^H = \bigcup_{k \geq 1} \mathscr{F}_k^H$. We can encode each element f of $\mathscr{F}^H$ with $c_H(f) = k + k^2$ bits, where the first k bits indicate the smallest k such that $f \in \mathscr{F}_k^H$ and the following k^2 bits encode the labels of each bin. This is a prefix encoding of all the elements in $\mathscr{F}^H$.

We define our estimator as
Equation:

$$\widehat{f}_n^H = \widehat{f}_n^{\widehat{k}},$$

where
Equation:

$$\widehat{f}_n^{(k)} = \arg\min_{f \in \mathscr{F}_k^H} \widehat{R}_n(f),$$

and
Equation:

$$\widehat{k} = \underset{k \geq 1}{\operatorname{argmin}} \left\{ \widehat{R}_n \left(\widehat{f}_n^{(k)} + \sqrt{\frac{\left(k + k^2\right) \log 2 + \frac{1}{2} \log n}{2n}} \right\} \right.$$

Therefore $\widehat{f}_n^H$ minimizes
Equation:

$$\widehat{R}_n(f) + \sqrt{\frac{c_H(f) \log 2 + \frac{1}{2} \log n}{2n}},$$

over all $f \in \mathscr{F}^H$. We showed before that
Equation:

$$E\left[R\left(\widehat{f}_n^H\right)\right] - R^* \leq \min_{f \in \mathscr{F}^H} \left\{ R(f) - R^* + \sqrt{\frac{c_H(f) \log 2 + \frac{1}{2} \log n}{2n}} \right\} + \frac{1}{\sqrt{n}}.$$

To proceed with our analysis we need to make some assumptions on the intrinsic difficulty of the problem. We will assume that the Bayes decision boundary is a “well-behaved” 1-dimensional set, in the sense that it has box-counting dimension one (see Appendix "Box Counting Dimension"). This implies that, for an histogram with k^2 bins, the Bayes decision boundary intersects less than Ck bins, where C is a constant that does not depend on k. Furthermore we assume that the marginal distribution of X satisfies $P_X(A) \leq K|A|$, for any measurable subset $A \subseteq [0,1]^2$. This means that the samples collected do not accumulate anywhere in the unit square.

Under the above assumptions we can conclude that
Equation:

$$\min_{f \in \mathscr{F}_k^H} R(f) - R^* \leq \frac{K}{k^2} Ck = \frac{CK}{k}.$$

Therefore

Equation:

$$E\left[R\left(\widehat{f}_n^H\right)\right] - R^* \;\leq\; CK/k + \sqrt{\frac{(k+k^2)\,\log 2 + \frac{1}{2}\,\log n}{2n}} + \frac{1}{\sqrt{n}}.$$

We can balance the terms in the right side of the above expression using $k = n^{1/4}$ (for n large) therefore
Equation:

$$E\left[R\left(\widehat{f}_n^H\right)\right] - R^* \;=\; O\left(n^{-1/4}\right), \quad \text{as } n \to \infty.$$

Dyadic Decision Trees

Now let's consider the dyadic decision trees, under the assumptions above, and contrast these with the histogram classifier. Let
Equation:

$$\mathscr{F}_k^T = \{\text{tree classifiers with } k \text{ leafs}\}.$$

Let $\mathscr{F}^T = \bigcup_{k\geq 1} \mathscr{F}_k^T$. We can prefix encode each element f of $\mathscr{F}^T$ with $c_T\left(f\right) = 3k - 1$ bits, as described before.

Let
Equation:

$$\widehat{f}_n^T = \widehat{f}_n^{\left(\widehat{k}\right)},$$

where
Equation:

$$\widehat{f}_n^{(k)} = \arg\min_{f\in\mathscr{F}_k^T} \widehat{R}_n\left(f\right),$$

and
Equation:

$$\widehat{k} = \operatorname*{argmin}_{k \geq 1} \left\{ \widehat{R}_n \left(\widehat{f}_n^{(k)} + \sqrt{\frac{(3k-1)\log 2 + \frac{1}{2}\log n}{2n}} \right\} \right.$$

Hence $\widehat{f}_n^T$ minimizes
Equation:

$$\widehat{R}_n(f) + \sqrt{\frac{c_T(f)\log 2 + \frac{1}{2}\log n}{2n}},$$

over all $f \in \mathscr{F}^T$. Moreover
Equation:

$$E\left[R\left(\widehat{f}_n^T\right)\right] - R^* \leq \min_{f \in \mathscr{F}^T} \left\{ R(f) - R^* + \sqrt{\frac{c_T(f)\log 2 + \frac{1}{2}\log n}{2n}} \right\} + \frac{1}{\sqrt{n}}.$$

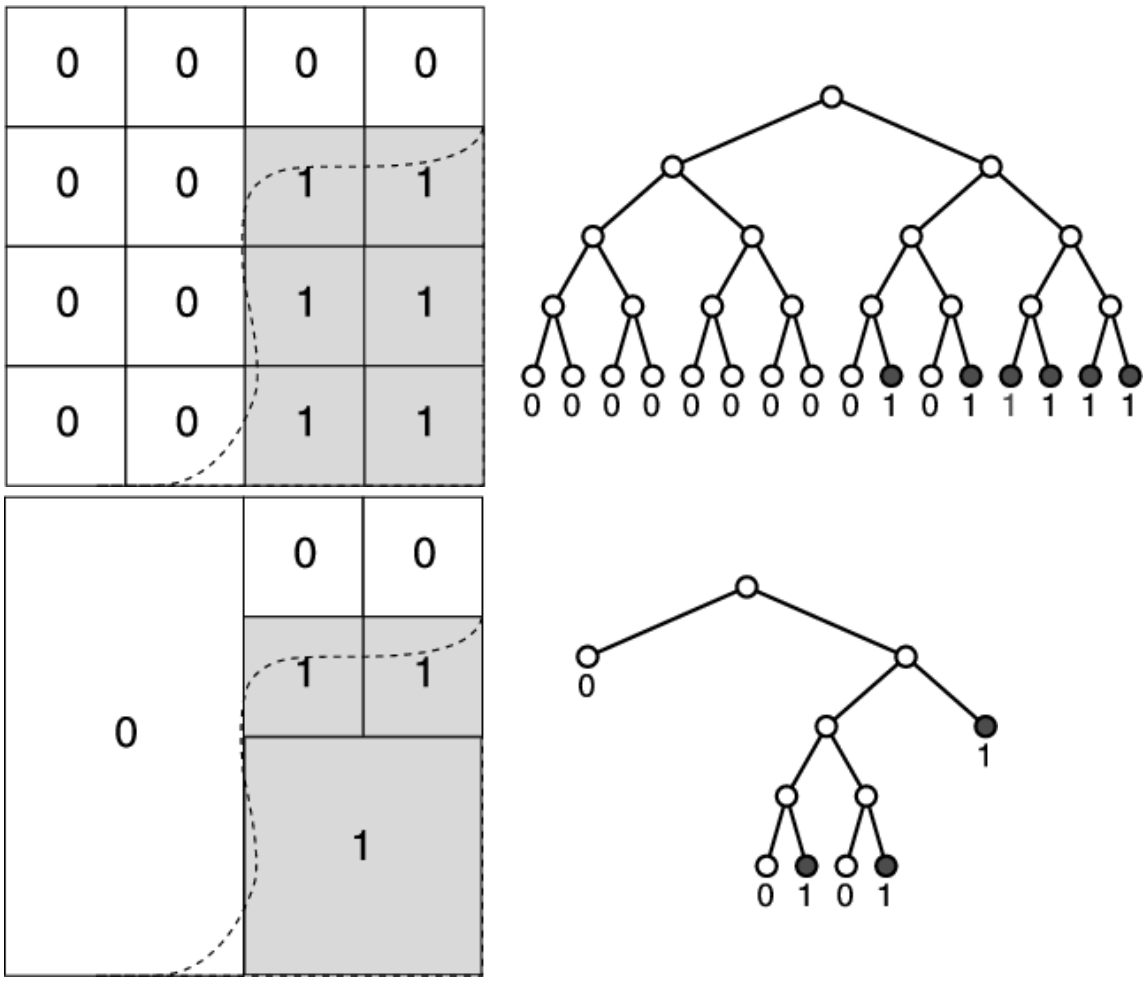
If the Bayes decision boundary is a 1-dimensional set, as in "Histogram Risk Bound", there exists a tree with at most $8Ck$ leafs such that the boundary is contained in at most Ck squares, each of volume $1/k^2$. To see this, start with a tree yielding the histogram partition with k^2 boxes (**i.e.,** the tree partitioning the unit square into k^2 equal sized squares). Now prune all the nodes that do not intersect the boundary. In [link] we illustrate the procedure. If you carefully bound the number of leafs you need at each level you can show that you will have in total less than $8Ck$ leafs. We conclude then that there exists a tree with at most $8Ck$ leafs that has the same risk as a histogram with $O\left(k^2\right)$ bins. Therefore, using [link] we have
Equation:

$$E\left[R\left(\widehat{f}_n^T\right)\right] - R^* \leq CK/k + \sqrt{\frac{(3(8Ck)-1)\log 2 + \frac{1}{2}\log n}{2n}} + \frac{1}{\sqrt{n}}.$$

We can balance the terms in the right side of the above expression using $k = n^{1/3}$ (for n large) therefore
Equation:

$$E\left[R\left(\widehat{f}_n^T\right)\right] - R^* \;=\; O\left(n^{-1/3}\right), \quad \text{as } n \to \infty.$$

Illustration of the tree pruning procedure: (a) Histogram classification rule, for a partition with 16 bins, and corresponding binary tree representation (with 16 leafs). (b) Pruned version of the histogram tree, yielding exactly the same classification rule, but now requiring only 6 leafs. (**Note:** The trees where constructed using the procedure of Figure)



Final Comments

Trees generally work much better than histogram classifiers. This is essentially because they provide much more efficient ways of approximating the Bayes decision boundary (as we saw in our example, under reasonable assumptions on the Bayes

boundary, a tree encoded with $O(k)$ bits can describe the same classifier as an histogram that requires $O\left(k^2\right)$ bits).

The dyadic decision trees studied here are different than classical tree rules, such as CART or C4.5. Those techniques select a tree according to
Equation:

$$\widehat{k} = \operatorname{argmin}_{k \geq 1} \left\{ \widehat{R}_n \left(\widehat{f}_n^{(k)} \right) + \alpha k \right\},$$

for some $\alpha > 0$ whereas ours was roughly
Equation:

$$\widehat{k} = \operatorname{argmin}_{k \geq 1} \left\{ \widehat{R}_n \left(\widehat{f}_n^{(k)} \right) + \alpha \sqrt{k} \right\},$$

for $\alpha \approx \sqrt{\frac{3 \log 2}{2n}}$. The square root penalty is essential for the risk bound. No such bound exists for CART or C4.5 . Moreover, recent experimental work has shown that the square root penalty often performs better in practice. Finally, recent results show that a slightly tighter bounding procedure for the estimation error can be used to show that dyadic decision trees (with a slightly different pruning procedure) achieve a rate of
Equation:

$$E\left[R\left(\widehat{f}_n^T\right)\right] - R^* \;=\; O\left(n^{-1/2}\right), \quad \text{as } n \to \infty,$$

which turns out to be the minimax optimal rate (i.e., under the boundary assumptions above, no method can achieve a faster rate of convergence to the Bayes error).

Box Counting Dimension

The notion of dimension of a sets arises in many aspects of mathematics, and it is particularly relevant to the study of fractals (that besides some important applications make really cool t-shirts). The dimension somehow indicates how we should measure the contents of a set (length, area, volume, etc...). The box-counting dimension is a simple definition of the dimension of a set. The main idea is to cover the set with boxes with sidelength r. Let $N(r)$ denote the smallest number of such boxes, then the box counting dimension is defined as

Equation:

$$\lim_{r \to 0} \frac{\log N(r)}{-\log r}.$$

Although the boxes considered above do not need to be aligned on a rectangular grid (and can in fact overlap) we can usually consider them over a grid and obtain an upper bound on the box-counting dimension. To illustrate the main ideas let's consider a simple example, and connect it to the classification scenario considered before.

Let $f : [0,1] \to [0,1]$ be a Lipschitz function, with Lipschitz constant L (**i.e.,** $|f(a) - f(b)| \leq L|a-b|, \ \forall a, b \in [0,1]$). Define the set
Equation:

$$A = \{x = (x_1, x_2) : x_2 = f(x_1)\},$$

that is, the set A is the graphic of function f.

Consider a partition with k^2 squared boxes (just like the ones we used in the histograms), the points in set A intersect at most $C'k$ boxes, with $C' = (1 + \lceil L \rceil)$ (and also the number of intersected boxes is greater than k). The sidelength of the boxes is $1/k$ therefore the box-counting dimension of A satisfies
Equation:

$$\begin{aligned} \dim_B(A) &\leq \lim_{1/k \to 0} \frac{\log C'k}{-\log(1/k)} \\ &= \lim_{k \to \infty} \frac{\log C' + \log(k)}{\log(k)} \\ &= 1. \end{aligned}$$

The result above will hold for any "normal" set $A \subseteq [0,1]^2$ that does not occupy any area. For most sets the box-counting dimension is always going to be an integer, but for some "weird" sets (called fractal sets) it is not an integer. For example, the Koch curve has box-counting dimension $\log(4)/\log(3) = 1.26186...$. This means that it is not quite as small as a 1-dimensional curve, but not as big as a 2-dimensional set (hence occupies no area).

To connect these concepts to our classification scenario consider a simple example. Let $\eta(x) = P(Y = 1 | X = x)$ and assume $\eta(x)$ has the form

Equation:

$$\eta(x) = \frac{1}{2} + x_2 - f(x_1), \quad \forall x \equiv (x_1, x_2) \in \mathscr{X},$$

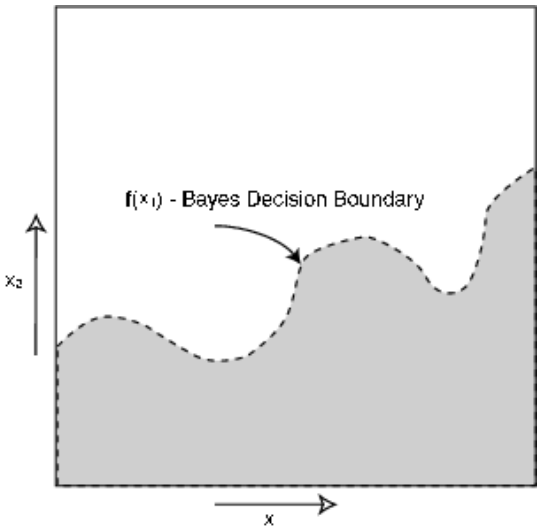
where $f : [0,1] \to [0,1]$ is Lipschitz with Lipschitz constant L. The Bayes classifier is then given by
Equation:

$$f^*(x) = \mathbf{1}_{\{\eta(x) \geq 1/2\}} \equiv \mathbf{1}_{\{x_2 \geq f(x_1)\}}.$$

This is depicted in [link]. Note that this is a special, restricted class of problems. That is, we are considering the subset of all classification problems such that the joint distribution P_{XY} satisfies $P(Y = 1|X = x) = 1/2 + x_2 - f(x_1)$ for some function f that is Lipschitz. The Bayes decision boundary is therefore given by
Equation:

$$A = \{x = (x_1, x_2) : x_2 = f(x_1)\}.$$

Has we observed before this set has box-counting dimension 1.



Bayes decision boundary for the setup described in Appendix .

Complexity Regularization for Squared Error Loss

Complexity Regularization in Regression

Recall the classification problem. In Lecture 6, where we assumed that $\min_{f \in \mathscr{F}} R(f) = 0$, we obtained the PAC bound $\forall f \in \mathscr{F}$
Equation:

$$\mathscr{P}\left\{R\left(\widehat{f}_n\right) > \epsilon\right\} \leq |\mathscr{F}| e^{-n\epsilon}.$$

From Corrolary 1 in Lecture 6,
Equation:

$$E\left[R\left(\widehat{f}_n\right)\right] \leq \frac{1+\log|\mathscr{F}|}{n}.$$

In Lectures 7 and 8, we dropped the assumption that $\min_{f \in \mathscr{F}} R(f) = 0$ and obtained, $\forall f \in \mathscr{F}$
Equation:

$$\mathscr{P}\left\{R\left(\widehat{f}_n\right) > \epsilon\right\} \leq |\mathscr{F}| e^{-2n\epsilon^2}.$$

This led to
Equation:

$$E\left[R\left(\widehat{f}_n\right) - \min_{f \in \mathscr{F}} R(f)\right] \leq \sqrt{\frac{\log|\mathscr{F}| + \log n + 2}{n}}.$$

Hoeffding's inequality was central to our analysis of learning under bounded loss functions. In many regression and signal estimation problems it is natural to consider squared error loss functions (rather than $0/1$ or absolute error). In such cases, we will need to derive bounds using different techniques.

Example:
To illustrate the distinction between classification and regression, consider a simple, scalar signal plus noise problem. Consider $Y_i = \theta + W_i$, $i = 1, \cdots, n$, where θ is a fixed unknown scalar parameter and the W_i are independent, zero-mean, unit variance random variables. Let $\overline{Y} = 1/n \sum_{i=1}^{n} Y_i$. Then, according to the Central Limit Theorem, $\overline{Y}$ is distributed approximately $N(\theta, 1/n)$. A simple tail-bound on the Gaussian distribution gives us
Equation:

$$P\left(\overline{Y} - \theta > \epsilon\right) = P\left(W > \epsilon\right) \;\leq\; \frac{1}{2} e^{-n\epsilon^2/2},$$

which implies that
Equation:

$$P(|\overline{Y} - \theta|^2 > \epsilon) \;\leq\; e^{-n\epsilon^2/2}.$$

This is a bound on the deviations of the squared error $\text{err}^2 = \left|\overline{Y} - \theta\right|^2$. Notice that the exponential decay rate is a function of ϵ rather than ϵ^2, as in Hoeffding's inequality. The squared error concentration inequality implies that $E[|\overline{Y} - \theta|^2] = O\left(\frac{1}{n}\right)$ (just write $E\left[\text{err}^2\right] = \int_0^\infty P\left(\text{err}^2 > t\right) dt$). Therefore, in regression with a squared error loss, we can hope to get a rate of convergence as fast as n^{-1} instead of $n^{-1/2}$. The reason is simply because we are using an squared error loss instead of the $0/1$ or absolute error loss.
To begin our investigation into regression and function estimation, let us consider the following. Let $\mathscr{X} = \mathbf{R}^d$ and $\mathscr{Y} = \mathbf{R}$. Take $\mathscr{F}$such that $f \in \mathscr{F}$ is a map $f : \mathbf{R}^d \mapsto \mathbf{R}$. We have training data $\{X_i, Y_i\}_{i=1}^n \overset{i.i.d.}{\sim} P_{XY}$. As our loss function, we take the squared error, **i.e.,**
Equation:

$$l\left(f\left(X_i\right), Y_i\right) = \left(f\left(X_i\right) - Y_i\right)^2.$$

The risk is then the MSE:
Equation:

$$R\left(f\right) = E\Big[\left(f\left(X\right) - Y\right)^2\Big].$$

We know that the function f^* that minimizes the MSE is just the conditional expectation of Y given X:
Equation:

$$f^* = E\left[Y|X = x\right].$$

Now let $R^* = R\left(f^*\right)$. We would like to select an $\widehat{f}_n \in \mathscr{F}$ using the training data $\{X_i, Y_i\}_{i=1}^n$ such that the **excess risk**
Equation:

$$E\left[R\left(\widehat{f}_n\right)\right] - R^* \geq 0$$

is small. Let's consider the difference between the empirical risks:
Equation:

$$\widehat{R}\left(f\right) - \widehat{R}\left(f^*\right) = \frac{1}{n}\sum_{i=1}^n \left(f\left(X_i\right) - Y_i\right)^2 - \frac{1}{n}\sum_{i=1}^n \left(f^*\left(X_i\right) - Y_i\right)^2.$$

Note that $E\left[\widehat{R}\left(f\right) - \widehat{R}\left(f^*\right)\right] = R\left(f\right) - R\left(f^*\right)$. Hence, by the Strong Law of Large Numbers (SLLN), we know that
Equation:

$$\widehat{R}\left(f\right) - \widehat{R}\left(f^*\right) \to R\left(f\right) - R\left(f^*\right)$$

as $n \to \infty$. But how fast is this convergence?
We will derive a PAC style bound for the difference $\widehat{R}\left(f\right) - \widehat{R}\left(f^*\right) - \left(R\left(f\right) - R\left(f^*\right)\right)$. The following derivation is from Barron 1991. The excess risk and it empirical counterpart will be denoted by
Equation:

$$\begin{aligned} r\left(f, f^*\right) &= R\left(f\right) - R\left(f^*\right) \\ \hat{r}\left(f, f^*\right) &= \widehat{R}\left(f\right) - \widehat{R}\left(f^*\right) \end{aligned}.$$

Note that $\hat{r}\left(f, f^*\right)$ is the sum of independent random variables:
Equation:

$$\hat{r}\left(f, f^*\right) = -\frac{1}{n}\sum_{i=1}^{n} U_i,$$

where $U_i = -\left(Y_i - f\left(X_i\right)\right)^2 + \left(Y_i - f^*\left(X_i\right)\right)^2$. Therefore,
$r\left(f, f^*\right) - \hat{r}\left(f, f^*\right) = \frac{1}{n}\sum_{i=1}^{n}\left(U_i - E\left[U_i\right]\right)$.
We are looking for a PAC bound of the form
Equation:

$$\mathscr{P}\left(r\left(f, f^*\right) - \hat{r}\left(f, f^*\right) > \epsilon\right) < \delta.$$

If the variables U_i are bounded, then we can apply Hoeffding's inequality. However, a more useful bound for our regression problem can be derived if the the variables U_i satisfy the following moment condition:
Equation:

$$E[\left|U_i - E\left[U_i\right]\right|^k] \leq \frac{var(U_i)}{2}\ k!\ h^{k-2}$$

for some $h > 0$.
The moment condition can be difficult to verify in general, but it does hold, for example, for bounded random variables. If [link] holds, then the Craig-Bernstein (CB) inequality states:
Equation:

$$\mathscr{P}\left(\frac{1}{n}\sum_{i=1}^{n}\left(U_i - E\left[U_i\right]\right) \geq \frac{t}{n\epsilon} + \frac{n\epsilon\ var\left(\frac{1}{n}\sum U_i\right)}{2(1-c)}\right) \leq e^{-t},$$

for $0 < \epsilon h \leq c < 1$ and $t > 0$. This shows that the tail decays exponentially in t, rather than exponentially in t^2. Recall Hoeffding's inequality:
Equation:

$$\mathscr{P}\left(\frac{1}{n}\sum_{i=1}^{n}\left(Z_i - E\left[Z_i\right]\right) \geq \frac{t}{n}\right) \leq e^{\frac{-2t^2}{n}}.$$

If $\frac{t}{n} \ll 1$, then $\frac{t^2}{n} \ll t$, which implies $e^{\frac{-2t^2}{n}} \gg e^{-t}$. This indicates that the CB inequality may be much tighter than Hoeffding's. To use the CB inequality, we need to bound the variance of $\frac{1}{n}\sum_{i=1}^{n} U_i$. Note that
Equation:

$$var\left(U_i\right) = var\left(-\left(Y_i - f\left(X_i\right)\right)^2 + \left(Y_i - f^*\left(X_i\right)\right)^2\right).$$

Assumption 1
The support of Y and the range f(X) is in a known interval of length b.

Proposition 1
With the above assumption, [link] holds with $h = \frac{2b^2}{3}$.

Proposition 2
Again, with the above assumption, it may be shown that
Equation:

$$var\left(U_i\right) \leq 5b^2 r\left(f, f^*\right).$$

You can write U_i as
Equation:

$$\begin{aligned} U_i &= 2Y_i f\left(X_i\right) - 2Y_i f^*\left(X_i\right) + f^*(X_i)^2 - f(X_i)^2 \\ &= 2Y_i f\left(X_i\right) - 2Y_i f^*\left(X_i\right) + 2f^*(X_i)^2 - f^*(X_i)^2 - f(X_i)^2 + 2f\left(X_i\right) f^*\left(X_i\right) - 2f\left(X_i\right) f^*\left(X_i\right) \\ &= 2\left(Y_i - f^*\left(X_i\right)\right)\left(f\left(X_i\right) - f^*\left(X_i\right)\right) - \left(f\left(X_i\right) - f^*\left(X_i\right)\right)^2 \end{aligned}.$$

Note that the variance of U_i is upper-bounded by its second moment. Also note that the covariance of the two terms above is zero:
Equation:

$$\begin{aligned} E\left[2\left(Y_i - f^*\left(X_i\right)\right)\left(f\left(X_i\right) - f^*\left(X_i\right)\right)\left(f\left(X_i\right) - f^*\left(X_i\right)\right)^2\right] &= E[T_1 T_2] \\ &= E_X\left[E_{Y|X}\left[T_1 T_2\right]\right] \\ &= E_X\left[T_2 E_{Y|X}\left[T_1\right]\right] \\ &= E_X\left[T_2 {}^* 0\right] \\ &= 0 \end{aligned}$$

This is evident when you recall that $f^*\left(X_i\right) = E\left[Y|X = X_i\right]$. Now we can bound the second moments of T_1 and T_2 :
Equation:

$$\begin{aligned} E[T_1] &= 4E\left[\left(\left(Y_i - f^*\left(X_i\right)\right)\left(f\left(X_i\right) - f^*\left(X_i\right)\right)\right)^2\right] \\ &= 4E\left[\left(Y_i - f^*\left(X_i\right)\right)^2\left(f\left(X_i\right) - f^*\left(X_i\right)\right)^2\right] \\ &\leq 4E\left[b^2\left(f\left(X_i\right) - f^*\left(X_i\right)\right)^2\right] \\ E[T_2] &= E\left[\left(f\left(X_i\right) - f^*\left(X_i\right)\right)^4\right] \\ &= E\left[\left(f\left(X_i\right) - f^*\left(X_i\right)\right)^2\left(f\left(X_i\right) - f^*\left(X_i\right)\right)^2\right] \\ &\leq E\left[b^2\left(f\left(X_i\right) - f^*\left(X_i\right)\right)^2\right] \end{aligned}.$$

So $var\left(U_i\right) \leq 5b^2 E\left[\left(f\left(X_i\right) - f^*\left(X_i\right)\right)^2\right]$. The final step is to see that
Equation:

$$r\left(f, f^*\right) = E\left[U_i\right] = E_X\left[E_{Y|X}\left[U_i\right]\right] = E\left[\left(f\left(X_i\right) - f^*\left(X_i\right)\right)^2\right].$$

Thus, $n\ var\left(\frac{1}{n}\sum_{i=1}^{n} U_i\right) \leq 5b^2 r\left(f, f^*\right)$. And therefore, we can say that, with probability at least $1 - e^{-t}$,
Equation:

$$r\left(f, f^*\right) - \hat{r}\left(f, f^*\right) \leq \frac{t}{n\ \epsilon} + \frac{5\epsilon\ b^2\ r\left(f, f^*\right)}{2(1-c)}.$$

In other words, with probability at least $1 - \delta$ (where $\delta = e^{-t}$),
Equation:

$$r\left(f, f^*\right) - \hat{r}\left(f, f^*\right) \leq \frac{\log\frac{1}{\delta}}{n\ \epsilon} + \frac{5\epsilon\ b^2\ r\left(f, f^*\right)}{2(1-c)}.$$

Now, suppose we have assigned positive numbers $c(f)$ to each $f \in \mathscr{F}$ satisfying the Kraft inequality:
Equation:

$$\sum_{f \in \mathscr{F}} 2^{-c(f)} \leq 1.$$

Note that [link] holds $\forall \delta > 0$. In particular, we let δ be a function of f:
Equation:

$$\delta\left(f\right) = 2^{-c(f)}\delta.$$

So we can use this δ along with the procedure introduced in Lecture 9 (**i.e.,** Union of events bound followed by the Kraft inequality) to obtain the following. For all $f \in \mathscr{F}$,$\forall \delta > 0$,
Equation:

$$r\left(f, f^*\right) - \hat{r}\left(f, f^*\right) \leq \frac{c\left(f\right)\log 2 + \log\frac{1}{\delta}}{n\ \epsilon} + \frac{5\epsilon\ b^2\ r\left(f, f^*\right)}{2(1-c)}$$

with probability at least $1 - \delta$. Now set $c = \epsilon\ h = \frac{2b^2\ \epsilon}{3}$ and assume $\epsilon < \frac{6}{19b^2}$. Then define
Equation:

$$\alpha = \frac{5\epsilon\ b^2}{2(1-c)} < 1.$$

Now, after using α and rearranging terms, we have:
Equation:

$$(1-\alpha) r\left(f, f^*\right) \leq \hat{r}\left(f, f^*\right) + \frac{c\left(f\right)\log 2 + \log\frac{1}{\delta}}{\epsilon\ n}.$$

We want to choose f to minmize this upper bound. So take
Equation:

$$\widehat{f}_n = \operatorname*{argmin}_{f \in \mathscr{F}} \left\{ \widehat{R}_n(f) + \frac{c(f) \log 2}{n\epsilon} \right\}.$$

So, with probability at least $1-\delta$,
Equation:

$$\begin{aligned} (1-\alpha) r\left(\widehat{f}_n, f^*\right) &\leq \hat{r}\left(\widehat{f}_n, f^*\right) + \frac{c\left(\widehat{f}_n\right) \log 2 + \log \frac{1}{\delta}}{\epsilon\ n} \\ &\leq \hat{r}\left(f_n^*, f^*\right) + \frac{c\left(f_n^*\right) \log 2 + \log \frac{1}{\delta}}{\epsilon\ n} \end{aligned}$$

where $f_n^* = \operatorname{argmin}_{f \in \mathscr{F}} \left\{ R(f) + \frac{c(f) \log 2}{n\epsilon} \right\}$.

Now we use the Craig-Bernstein inequality to bound the difference between $\hat{r}\left(f_n^*, f^*\right)$ and $r\left(f_n^*, f^*\right)$: With probability at least $1-\delta$,
Equation:

$$\hat{r}\left(f_n^*, f^*\right) \leq r\left(f_n^*, f^*\right) + \alpha\ r\left(f_n^*, f^*\right) + \frac{\log\left(\frac{1}{\delta}\right)}{n\epsilon}.$$

Now we can again use the union bound to combine [link] and [link]: With probability at least $1-2\delta, \forall \delta > 0$,
Equation:

$$r\left(\widehat{f}_n, f^*\right) \leq \frac{1+\alpha}{1-\alpha} r\left(f_n^*, f^*\right) + \frac{c\left(f_n^*\right) \log 2 + 2 \log 1/\delta}{n\epsilon}.$$

Now set $\delta = e^{\frac{-n\epsilon t}{2}}$, then we have
Equation:

$$\mathscr{P}\left(r\left(\widehat{f}_n, f^*\right) - \frac{1+\alpha}{1-\alpha} r\left(f_n^*, f^*\right) + \frac{c\left(f_n^*\right) \log 2}{n\epsilon} \geq t \right) \leq 2e^{\frac{-n\epsilon t}{2}}.$$

Integrating, we get
Equation:

$$\begin{aligned} E\left[r\left(\widehat{f}_n, f^*\right) - \frac{1+\alpha}{1-\alpha} r\left(f_n^*, f^*\right) + \frac{c\left(f_n^*\right) \log 2}{n\epsilon} \right] &\leq \int_0^\infty \mathscr{P}(\ \text{//} \geq t)\ dt \\ &\leq \int_0^\infty 2e^{\frac{-n\epsilon t}{2}} \qquad . \\ &= \frac{4}{n\epsilon} \end{aligned}$$

To sum up, we have shown that for $\epsilon < \frac{6}{19b^2}$,
Equation:

$$E\left[r\left(\widehat{f}_n, f^*\right)\right] \leq \left(\frac{1+\alpha}{1-\alpha}\right) r\left(f_n^*, f^*\right) + \frac{c\left(f_n^*\right) \log 2 + 4}{n\epsilon},$$

or,
Equation:

$$E\left[r\left(\widehat{f}_n, f^*\right)\right] \leq \left(\frac{1+\alpha}{1-\alpha}\right) \min_{f \in \mathscr{F}} \left\{r\left(f, f^*\right) + \frac{c(f) \log 2}{n\epsilon}\right\} + \frac{4}{n\epsilon},$$

since $\alpha < 1$. Or, in expanded form:
Equation:

$$E\left[R\left(\widehat{f}_n\right)\right] - R\left(f^*\right) \;\leq\; \left(\frac{1+\alpha}{1-\alpha}\right) \min_{f \in \mathscr{F}} \left\{R\left(f\right) - R\left(f^*\right) + \frac{c(f) \log 2}{n\epsilon}\right\} + \frac{4}{n\epsilon}.$$

Notice that if $f^* \in \mathscr{F}$ and if $c\left(f^*\right)$ is not too large (e.g., $c\left(f^*\right) \approx$log n), then we have
$E\left[R\left(\widehat{f}_n\right)\right] - R\left(f^*\right) = O\left(n^{-1} \log n\right)$, within a logarithmic factor of the parametric rate of convergence!

Maximum Likelihood Estimation

In the last lecture we derived a risk (MSE) bound for regression problems; i.e., select an $f \in \mathscr{F}$ so that $E\left[\left(f\left(X\right)-Y\right)^2\right]-E\left[\left(f^*\left(X\right)-Y\right)^2\right]$ is small, where $f^*\left(x\right)=E\left[Y|X=x\right]$. The result is summarized below.

Theorem

Complexity Regularization with Squared Error Loss

Let $\mathscr{X}=\mathbb{R}^d$, $\mathscr{Y}=[-b/2,b/2]$, $\{X_i,Y_i\}_{i=1}^n$ iid, P_{XY} unknown, $\mathscr{F}$ = {collection of candidate functions},

Equation:

$$f:\mathbb{R}^d\to\mathscr{Y},\quad R\left(f\right)=E\left[\left(f\left(X\right)-Y\right)^2\right].$$

Let $c(f)$, $f\in\mathscr{F}$, be positive numbers satisfying $\sum_{f\in\mathscr{F}}2^{-c(f)}\leq 1$, and select a function from $\mathscr{F}$ according to

Equation:

$$\widehat{f}_n=\text{argmin}\left\{\widehat{R}_n\left(f\right)+\frac{1}{\epsilon}\,\frac{c(f)\,\log 2}{n}\right\},$$

with $\epsilon\leq\frac{3}{5b^2}$ and $\widehat{R}_n\left(f\right)=\frac{1}{n}\sum_{i=1}^n\left(f\left(X_i\right)-Y_i\right)^2$. Then,

Equation:

$$E\left[R\left(\widehat{f}_n\right)\right]-R\left(f^*\right)\;\leq\;\left(\frac{1+\alpha}{1-\alpha}\right)\min_{f\in\mathscr{F}}\left\{R\left(f\right)-R\left(f^*\right)+\frac{1}{\epsilon}\,\frac{c(f)\,\log 2}{n}\right\}+O\left(n^{-1}\right)$$

where $\alpha=\frac{\epsilon b^2}{1-2b^2\epsilon/3}$.

Maximum Likelihood Estimation

The focus of this lecture is to consider another approach to learning based on maximum likelihood estimation. Consider the classical signal plus noise model:

Equation:

$$Y_i=f\left(\frac{i}{n}\right)+W_i,i=1,\cdots,n$$

where W_i are iid zero-mean noises. Furthermore, assume that $W_i\sim P\left(w\right)$ for some known density $P(w)$. Then

Equation:

$$Y_i \sim P\left(y - f\left(\frac{i}{n}\right)\right) \equiv P_{f_i}(y)$$

since $Y_i - f\left(\frac{i}{n}\right) = W_i$.

A very common and useful loss function to consider is
Equation:

$$\widehat{R}_n(f) = \frac{1}{n}\sum_{i=1}^{n}(-\log P_{f_i}(Y_i)).$$

Minimizing $\widehat{R}_n$ with respect to f is equivalent to maximizing
Equation:

$$\frac{1}{n}\sum_{i=1}^{n}\log P_{f_i}(Y_i)$$

or
Equation:

$$\prod_{i=1}^{n} P_{f_i}(Y_i).$$

Thus, using the negative log-likelihood as a loss function leads to maximum likelihood estimation. If the W_i are iid zero-mean Gaussian r.v.s then this is just the squared error loss we considered last time. If the W_i are Laplacian distributed e.g. $P(w) \propto e^{-|w|}$, then we obtain the absolute error, or L_1, loss function. We can also handle non-additive models such as the Poisson model
Equation:

$$Y_i \sim P(y|f(i/n)) = e^{-f(i/n)}\frac{[f(i/n)]^y}{y!}.$$

In this case
Equation:

$$-\log P(Y_i|f(i/n)) \;=\; f(i/n) - Y_i \log\left(f(i/n)\right) + \text{constant}$$

which is a very different loss function, but quite appropriate for many imaging problems.

Before we investigate maximum likelihood estimation for model selection, let's review some of the basic concepts. Let Θ denote a parameter space (e.g., $\Theta = R$), and assume we have observations
Equation:

$$Y_i \overset{iid}{\sim} P_{\theta^*}(y), \quad i = 1, \cdots, n$$

where $\theta^* \in \Theta$ is a parameter determining the density of the $\{Y_i\}$. The ML estimator of θ^* is
Equation:

$$\begin{aligned} \hat{\theta}_n &= \underset{\theta \in \Theta}{\text{argmax}} \prod_{i=1}^{n} P_\theta(Y_i) \\ &= \underset{\theta \in \Theta}{\text{argmax}} \sum_{i=1}^{n} \log P_\theta(Y_i) \\ &= \underset{\theta \in \Theta}{\text{argmin}} \sum_{i=1}^{n} -\log P_\theta(Y_i). \end{aligned}$$

$\hat{\theta}$ maximizes the expected log-likelihood. To see this, let's compare the expected log-likelihood of θ^* with any other $\theta \in \Theta$.
Equation:

$$\begin{aligned} E[\log P_{\theta^*}(Y) - \log P_\theta(Y)] &= E\left[\log \frac{P_{\theta^*}(Y)}{P_\theta(Y)}\right] \\ &= \int \log \frac{P_{\theta^*}(y)}{P_\theta(y)} P_{\theta^*}(y) dy \\ &= K(P_\theta, P_{\theta^*}) \quad \text{the KL divergence} \\ &\geq 0 \quad \text{with equality iff } P_{\theta^*} = P_\theta. \end{aligned}$$

Why?
Equation:

$$\begin{aligned} -E\left[\log \frac{P_{\theta^*}(y)}{P_\theta(y)}\right] &= E\left[\log \frac{P_\theta(y)}{P_{\theta^*}(y)}\right] \\ &\leq \log E\left[\frac{P_\theta(y)}{P_{\theta^*}(y)}\right] \\ &= \log \int P_\theta(y) dy = 0 \\ &\Rightarrow K(P_\theta, P_{\theta^*}) \geq 0 \end{aligned}$$

On the other hand, since $\hat{\theta}_n$ maximizes the likelihood over $\theta \in \Theta$, we have
Equation:

$$\sum_{i=1}^{n} \log \frac{P_{\theta^*}(Y_i)}{P_{\hat{\theta}_n}(Y_i)} = \sum_{i=1}^{n} \log P_{\theta^*}(Y_i) - \log P_{\hat{\theta}_n}(Y_i) \leq 0.$$

Therefore,
Equation:

$$\frac{1}{n} \sum_{i=1}^{n} \log \frac{P_{\theta^*}(Y_i)}{P_{\hat{\theta}_n}(Y_i)} - K\left(P_{\hat{\theta}_n}, P_{\theta^*}\right) + K\left(P_{\hat{\theta}_n}, P_{\theta^*}\right) \leq 0$$

or re-arranging
Equation:

$$K\left(P_{\hat{\theta}_n}, P_{\theta^*}\right) \leq \left| \frac{1}{n} \sum_{i=1}^{n} \log \frac{P_{\theta^*}(Y_i)}{P_{\hat{\theta}_n}(Y_i)} - K\left(P_{\hat{\theta}_n}, P_{\theta^*}\right) \right|.$$

Notice that the quantity
Equation:

$$\frac{1}{n} \sum_{i=1}^{n} \log \frac{P_{\theta^*}(Y_i)}{P_{\theta}(Y_i)}$$

is an empirical average whose mean is $K(P_\theta, P_{\theta^*})$. By the law of large numbers, for each $\theta \in \Theta$,
Equation:

$$\left| \frac{1}{n} \sum_{i=1}^{n} \log \frac{P_{\theta^*}(Y_i)}{P_{\theta}(Y_i)} - K\left(P_\theta, P_{\theta^*}\right) \right| \overset{a.s.}{\to} 0.$$

If this also holds for the sequence $\left\{\hat{\theta}_n\right\}$, then we have
Equation:

$$K\left(P_{\hat{\theta}_n}, P_{\theta^*}\right) \leq \left| \frac{1}{n} \sum \log \frac{P_{\theta^*}(Y_i)}{P_{\hat{\theta}_n}(Y_i)} - K\left(P_{\hat{\theta}_n}, P_{\theta^*}\right) \right| \to 0 \text{ as } n \to \infty$$

which implies that
Equation:

$$P_{\hat{\theta}_n} \to P_{\theta^*}$$

which often implies that
Equation:

$$\hat{\theta}_n \to \theta^*$$

in some appropriate sense (e.g., point-wise or in norm).

Example:
Gaussian Distributions
Equation:

$$P_{\theta^*}(y) = \frac{1}{\sqrt{\pi}} e^{-\left(y-\theta^*\right)^2}$$

Equation:

$$\Theta = \mathbb{R}, \quad \{Y_i\}_{i=1}^n \overset{iid}{\sim} P_{\theta^*}(y)$$

Equation:

$$\begin{aligned} K(P_\theta, P_{\theta^*}) &= \int \log \frac{P_{\theta^*}(y)}{P_\theta(y)} P_{\theta^*}(y) dy \\ &= \int \left[(y-\theta)^2 - \left(y-\theta^*\right)^2 \right] P_{\theta^*}(y) dy \\ &= E_{\theta^*}\left[(y-\theta)^2\right] - E_{\theta^*}\left[\left(y-\theta^*\right)^2\right] \\ &= E_{\theta^*}\left[Y^2 - 2Y\theta + \theta^2\right] - 1/2 \\ &= \left(\theta^*\right)^2 + 1/2 - 2\theta^*\theta + \theta^2 - 1/2 \\ &= \left(\theta^* - \theta\right)^2 \end{aligned}$$

Equation:

$$\Rightarrow \theta^* \text{ maximizes } E\left[\log P_\theta(Y)\right] \text{ wrt } \theta \in \Theta$$

Equation:

$$\begin{aligned}\hat{\theta}_n &= \operatorname{argmax}_{\theta} \left\{ -\sum (Y_i - \theta)^2 \right\} \\ &= \operatorname{argmin}_{\theta} \left\{ \sum (Y_i - \theta)^2 \right\} \\ &= \frac{1}{n} \sum_{i=1}^{n} Y_i\end{aligned}$$

Hellinger Distance

The KL divergence is not a distance function.
Equation:

$$K\left(P_{\theta_1}, P_{\theta_2}\right) \neq K\left(P_{\theta_2}, P_{\theta_1}\right)$$

Therefore, it is often more convenient to work with the Hellinger metric,
Equation:

$$H\left(P_{\theta_1}, P_{\theta_2}\right) = \left(\int \left(P_{\theta_1}^{\frac{1}{2}} - P_{\theta_2}^{\frac{1}{2}} \right)^2 dy \right)^{\frac{1}{2}}.$$

The Hellinger metric is symmetric, non-negative and
Equation:

$$H\left(P_{\theta_1}, P_{\theta_2}\right) = H\left(P_{\theta_2}, P_{\theta_1}\right)$$

and therefore it is a distance measure. Furthermore, the squared Hellinger distance lower bounds the KL divergence, so convergence in KL divergence implies convergence of the Hellinger distance.

Proposition 1
Equation:

$$H^2\left(P_{\theta_1}, P_{\theta_2}\right) \leq K\left(P_{\theta_1}, P_{\theta_2}\right)$$

Proof:
Equation:

$$
\begin{aligned}
H(P_{\theta_1}, P_{\theta_2}) &= \int \left(\sqrt{P_{\theta_1}(y)} - \sqrt{P_{\theta_2}(y)}\right)^2 dy \\
&= \int P_{\theta_1}(y)dy + \int P_{\theta_2}(y)dy - 2\int \sqrt{P_{\theta_1}(y)}\sqrt{P_{\theta_2}(y)}dy \\
&= 2 - 2\int \sqrt{P_{\theta_1}(y)}\sqrt{P_{\theta_2}(y)}dy, \quad \text{since } \int P_\theta(y)dy = 1 \,\forall\theta \\
&= 2\left(1 - E_{\theta_2}\left[\sqrt{P_{\theta_1}(Y)/P_{\theta_2}(Y)}\right]\right) \\
&\leq 2\log\left(E_{\theta_2}\left[\sqrt{P_{\theta_2}(Y)/P_{\theta_1}(Y)}\right]\right), \quad \text{since} \, 1 - x \leq -\log x \\
&\leq 2E_{\theta_2}\left[\log\sqrt{P_{\theta_2}(Y)/P_{\theta_1}(Y)}\right], \quad \text{by Jensen's inequality} \\
&= E_{\theta_2}[\log(P_{\theta_2}(Y)/P_{\theta_1}(Y))] \equiv K(P_{\theta_1}, P_{\theta_2})
\end{aligned}
$$

Note that in the proof we also showed that
Equation:

$$
H(P_{\theta_1}, P_{\theta_2}) = 2\left(1 - \int \sqrt{P_{\theta_1}(y)}\sqrt{P_{\theta_2}(y)}dy\right)
$$

and using the fact $\log x \leq x - 1$ again, we have
Equation:

$$
H(P_{\theta_1}, P_{\theta_2}) \leq -2\log\left(\int \sqrt{P_{\theta_1}(y)}\sqrt{P_{\theta_2}(y)}dy\right).
$$

The quantity inside the log is called the **affinity** between P_{θ_1} and P_{θ_2}:
Equation:

$$
A(P_{\theta_1}, P_{\theta_2}) = \int \sqrt{P_{\theta_1}(y)}\sqrt{P_{\theta_2}(y)}dy.
$$

This is another measure of closeness between P_{θ_1} and P_{θ_2}.

Example:
Gaussian Distributions
Equation:

$$
P_\theta(y) = \frac{1}{\pi}e^{-(y-\theta)^2}
$$

Equation:

$$\begin{aligned} & -2\log\int\sqrt{P_{\theta_1}(y)}\sqrt{P_{\theta_2}(y)}dy \\ = & -2\log\int\left(\frac{1}{\sqrt{\pi}}e^{-(y-\theta_1)^2}\right)^{\frac{1}{2}}\left(\frac{1}{\sqrt{\pi}}e^{-(y-\theta_2)^2}\right)^{\frac{1}{2}}dy \\ = & -2\log\left(\int\frac{1}{\sqrt{\pi}}e^{-\left[\frac{(y-\theta_1)^2}{2}+\frac{(y-\theta_2)^2}{2}\right]}dy\right) \\ = & -2\log\left(\int\frac{1}{\sqrt{\pi}}e^{-\left[\left(y-\left(\frac{\theta_1+\theta_2}{2}\right)\right)^2+\left(\frac{\theta_1-\theta_2}{2}\right)^2\right]}dy\right) \\ = & -2\log e^{-\left(\frac{\theta_1-\theta_2}{2}\right)^2} \\ = & \frac{1}{2}(\theta_1-\theta_2)^2 \end{aligned}$$

Equation:

$$\begin{aligned} \Rightarrow & \quad -2\log A(P_{\theta_1},P_{\theta_2})=\frac{1}{2}(\theta_1-\theta_2)^2 \quad \text{for Gaussian distributions} \\ \Rightarrow & \quad H(P_{\theta_1},P_{\theta_2})\leq\frac{1}{2}(\theta_1-\theta_2)^2 \quad \text{for Gaussian.} \end{aligned}$$

Example:
Poisson Distributions
If $P_\theta(y)=e^{-\theta}\frac{\theta^y}{y!},\theta\geq 0$, then
Equation:

$$-2\log A(P_{\theta_1},P_{\theta_2})=\left(\sqrt{\theta_1}-\sqrt{\theta_2}\right)^2.$$

Equation:

Summary

$$Y_i\overset{iid}{\sim}P_{\theta^*}$$

1. Maximum likelihood estimator maximizes the empirical average
   Equation:

$$\frac{1}{n}\sum_{i=1}^{n}\log P_\theta(Y_i)$$

(our empirical risk is negative log-likelihood)

2. θ^* maximizes the expectation
   Equation:

$$E\left[\frac{1}{n}\sum_{i=1}^{n}\log P_\theta\left(Y_i\right)\right]$$

   (the risk is the expected negative log-likelihood)
3. **Equation:**

$$\frac{1}{n}\sum_{i=1}^{n}\log P_\theta\left(Y_i\right)\overset{a.s.}{\to}E\left[\frac{1}{n}\sum_{i=1}^{n}\log P_\theta\left(Y_i\right)\right]$$

   so we expect some sort of concentration of measure.
4. In particular, since
   Equation:

$$\frac{1}{n}\sum_{i=1}^{n}\log\frac{P_{\theta^*}\left(Y_i\right)}{P_\theta\left(Y_i\right)}\overset{a.s.}{\to}K\left(P_\theta,P_{\theta^*}\right)$$

   we might expect that $K\left(P_{\hat{\theta}_n},P_{\theta^*}\right)\to 0$ for the sequence of estimates $\left\{P_{\hat{\theta}_n}\right\}_{n=1}^{\infty}$.

So, the point is that maximum likelihood estimator is just a special case of a loss function in learning. Due to its special structure, we are naturally led to consider KL divergences, Hellinger distances, and Affinities.

Maximum Likelihood and Complexity Regularization

Review : Maximum Likelihood Estimation

In the last lecture, we have n i.i.d observations drawn from an unknown distribution
Equation:

$$Y_i \overset{i.i.d.}{\sim} p_{\theta^*} \quad , \ i = \{1, ..., n\}$$

Equation:

$$\text{where } \theta^* \in \Theta.$$

With **loss function** defined as $l(\theta, Y_i) = -\log p_\theta(Y_i)$, the empirical risk is
Equation:

$$\widehat{R_n} = -\frac{1}{n}\sum_{i=1}^{n} \log p_\theta(Y_i).$$

Essentially, we want to choose a distribution from the collection of distributions within the parameter space that minimizes the empirical risk,**i.e.,** we would like to select
Equation:

$$p_{\widehat{\theta_n}} \in \mathscr{P} = \{p_\theta\}_{\theta \in \Theta}$$

where
Equation:

$$\widehat{\theta_n} = \arg\min_{\theta \in \Theta} \quad -\sum_{i=1}^{n} \log p_\theta(Y_i).$$

The risk is defined as
Equation:

$$R(\theta) = E[l(\theta, Y)] = -E[\log p_\theta(Y)].$$

Note that θ^* minimizes $R(\theta)$ over Θ.
Equation:

$$\begin{aligned} \theta^* &= \arg\min_{\theta \in \Theta} \quad -E[\log p_\theta(Y)] \\ &= \operatorname{argmin}_{\theta \in \Theta} \quad -\int \log p_\theta(y) \cdot p_{\theta^*}(y)\, \mathrm{d}y. \end{aligned}$$

Finally, the excess risk of θ is defined as
Equation:

$$R(\theta) - R\left(\theta^*\right) = \int \log \frac{p_{\theta^*}(y)}{p_\theta(y)}\, p_{\theta^*}(y)\, \mathrm{d}y \equiv K\left(p_\theta, p_{\theta^*}\right).$$

We recognized that the excess risk corresponding to this loss function is simply the **Kullback-Leibler (KL) Divergence** or **Relative Entropy**, denoted by $K(p_{\theta_1}, p_{\theta_2})$. It is easy to see that $K(p_{\theta_1}, p_{\theta_2})$ is always non-negative and is zero if and only if $p_{\theta_1} = p_{\theta_2}$. KL divergence measures how different two probability distributions are and therefore is natural to measure convergence of the maximum likelihood procedures. However, $K(p_{\theta_1}, p_{\theta_2})$ is not a distance metric because it is not symmetric and does not satisfy the triangle inequality. For this reason, two other quantities play a key role in maximum likelihood estimation, namely **Hellinger Distance** and **Affinity**.

The Hellinger distance is defined as
Equation:

$$H\left(p_{\theta_1}, p_{\theta_2}\right) = \left(\int \left(\sqrt{p_{\theta_1}(y)} - \sqrt{p_{\theta_2}(y)}\right)^2 \mathrm{d}y\right)^{\frac{1}{2}}.$$

We proved that the squared Hellinger distance lower bounds the KL divergence:
Equation:

$$\begin{aligned} H^2\left(p_{\theta_1}, p_{\theta_2}\right) &\leq K(p_{\theta_1}, p_{\theta_2}) \\ H^2\left(p_{\theta_1}, p_{\theta_2}\right) &\leq K(p_{\theta_2}, p_{\theta_1}). \end{aligned}$$

The affinity is defined as
Equation:

$$A\left(p_{\theta_1}, p_{\theta_2}\right) = \int \sqrt{p_{\theta_1} \cdot p_{\theta_2}(y)}\, \mathrm{d}y.$$

we also proved that
Equation:

$$H^2\left(p_{\theta_1}, p_{\theta_2}\right) \leq -2 \log\left(A(p_{\theta_1}, p_{\theta_2})\right).$$

Example:
Gaussian Distribution
Y is Gaussian with mean θ and variance σ^2.
Equation:

$$p_\theta(y) = \frac{1}{\sqrt{2\pi\sigma^2}} e^{-\frac{(y-\theta)^2}{2\sigma^2}}.$$

First, look at
Equation:

$$\log \frac{p_{\theta_2}}{p_{\theta_1}} = \frac{1}{2\sigma^2}\left[\left(\theta_1^2 - \theta_2^2\right) - 2(\theta_1 - \theta_2)y\right].$$

Then,
Equation:

$$
\begin{aligned}
K(p_{\theta_1}, p_{\theta_2}) &= E_{\theta_2}\left[\log\ \frac{p_{\theta_2}}{p_{\theta_1}}\right] \\
&= \frac{\theta_1^2-\theta_2^2}{2\sigma^2} - \frac{2(\theta_1-\theta_2)}{2\sigma^2}\underbrace{\int y\cdot p_{\theta_2}(y)\,\mathrm{d}y}_{E[Y]=\theta_2} \\
&= \frac{1}{2\sigma^2}\left(\theta_1^2+\theta_2^2-2\theta_1\theta_2\right) \quad = \frac{\left(\theta_1^2-\theta_2\right)^2}{2\sigma^2}. \\
-2\log\ A(p_{\theta_1}, p_{\theta_2}) &= -2\log\left(\int\left(\frac{1}{\sqrt{2\pi\sigma^2}}\,e^{-\frac{(y-\theta_1)^2}{2\sigma^2}}\right)^{1/2}\cdot\left(\frac{1}{\sqrt{2\pi\sigma^2}}e^{-\frac{(y-\theta_2)^2}{2\sigma^2}}\right)^{1/2}\mathrm{d}y\right) \\
&= -2\log\left(\int\frac{1}{\sqrt{2\pi\sigma^2}}e^{-\frac{(y-\theta_1)^2}{4\sigma^2}-\frac{(y-\theta_2)^2}{4\sigma^2}}\,\mathrm{d}y\right) \\
&= -2\log\left(\int\frac{1}{\sqrt{2\pi\sigma^2}}e^{-\frac{1}{2\sigma^2}\left[\left(y-\frac{\theta_1+\theta_2}{2}\right)^2+\left(\frac{\theta_1-\theta_2}{2}\right)^2\right]}\,\mathrm{d}y\right) \\
&= -2\log\ e^{-\frac{\left(\frac{\theta_1-\theta_2}{2}\right)^2}{2\sigma^2}} \\
&= \frac{(\theta_1-\theta_2)^2}{4\sigma^2} \quad = \frac{1}{2}K\left(p_{\theta_1}, p_{\theta_2}\right) \quad \geq H^2\left(p_{\theta_1}, p_{\theta_2}\right).
\end{aligned}
$$

Maximum likelihood estimation and Complexity regularization

Suppose that we have n i.i.d training samples, $\{X_i, Y_i\}_{i=1}^n \overset{i.i.d.}{\sim} p_{XY}$.

Using conditional probability, p_{XY} can be written as
Equation:

$$p_{XY}(x,y) = p_X(x)\cdot p_{Y|X=x}(y).$$

Let's assume for the moment that p_X is completely unknown, but $p_{Y|X=x}(y)$ has a special form:
Equation:

$$p_{Y|X=x}(y) = p_{f^*(x)}(y)$$

where $p_{Y|X=x}(y)$ is a known parametric density function with parameter $f^*(x)$.

Example:
Signal-plus-noise observation model
Equation:

$$Y_i = f^*(X_i) + W_i \quad , i = 1, ..., n$$

where $W_i \overset{i.i.d.}{\sim} \mathcal{N}\left(0, \sigma^2\right)$ and $X_i \overset{i.i.d.}{\sim} p_X$.
Equation:

$$p_{f^*(x)}\left(y\right)=\frac{1}{\sqrt{2\pi\sigma^2}}e^{-\frac{\left(y-f^*(x)\right)^2}{2\sigma^2}}$$

$Y|X=x\sim\text{Poisson}\left(f^*\left(x\right)\right)$
Equation:

$$p_{f^*(x)}\left(y\right)=e^{-f^*(x)}\frac{\left[f^*\left(x\right)\right]^y}{y!}\,.$$

The likelihood loss function is
Equation:

$$\begin{aligned}l(f(x),y) &= -\log\ p_{XY}\left(X,Y\right)\\ &= -\log\ p_X\left(X\right)-\log\ p_{Y|X}\left(Y|X\right)\\ &= -\log\ p_X\left(X\right)-\log\ p_{f(X)}\left(Y\right).\end{aligned}$$

The **expected loss** is
Equation:

$$\begin{aligned}E[l(f(X),Y)] &= E_X\left[E_{Y|X}\left[l\left(f\left(X\right),Y\right)|X=x\right]\right]\\ &= E_X\left[\,E_{Y|X}\left[-\log\ p_X\left(x\right)-\log\ p_{f(x)}\left(Y\right)\middle|X=x\right]\,\right]\\ &= -E_X\left[\log\ p_X\left(X\right)\right]-E_X\left[\,E_{Y|X}\left[\log\ p_{f(x)}\left(Y\right)\middle|X=x\,\right]\,\right]\\ &= -E_X\left[\log\ p_X\left(X\right)\right]-E\left[\log\ p_{f(X)}\left(Y\right)\right].\end{aligned}$$

Notice that the first term is a constant with respect to f.
Hence, we define our risk to be
Equation:

$$\begin{aligned}R(f) &= -E\left[\log\ p_{f(X)}\left(Y\right)\right]\\ &= -E_X\left[\,E_{Y|X}\left[\log\ p_{f(x)}\left(Y\right)\middle|X=x\right]\,\right]\\ &= -\int\left(\int\log\ p_{f(x)}\left(y\right)\cdot p_{f^*(x)}\left(y\right)\mathrm{d}y\right)p_X\left(x\right)\mathrm{d}x\,.\end{aligned}$$

The function f^* minimizes this risk since $f\left(x\right)=f^*\left(x\right)$ minimizes the integrand.
Our empirical risk is the negative log-likelihood of the training samples:
Equation:

$$\widehat{R_n}\left(f\right)=\frac{1}{n}\sum_{i=1}^{n}-\log\ p_{f(X_i)}\left(Y_i\right).$$

The value $\frac{1}{n}$ is the **empirical** probability of observing $X=X_i$.
Often in function estimation, we have control over where we sample X. Let's assume that $\mathscr{X}=[0,1]^d$ and $\mathscr{Y}=\mathbf{R}$. Suppose we sample $\mathscr{X}$ uniformly with $n=m^d$ samples for some positive integer m (**i.e.,** ,take m evenly spaced samples in each coordinate).
Let x_i ,$i=1,...,n$ denote these sample points, and assume that $Y_i\sim p_{f^*(x_i)}\left(y\right)$. Then, our empirical risk is
Equation:

$$\widehat{R_n}\left(f\right)=\frac{1}{n}\sum_{i=1}^{n}l\left(f\left(x_i\right),Y_i\right)=\frac{1}{n}\sum_{i=1}^{n}-\log\ p_{f(x_i)}\left(Y_i\right).$$

Note that x_i is now a deterministic quantity.

Our risk is
Equation:

$$\begin{aligned} R(f) &= -\frac{1}{n}\sum_{i=1}^{n} E\left[\log\ p_{f(x_i)}\left(Y_i\right)\right] \\ &= -\frac{1}{n}\sum_{i=1}^{n}\left[\int \log\ p_{f(x_i)}\left(y_i\right)\cdot p_{f^*(x_i)}\left(y_i\right)\mathrm{d}y_i\right]. \end{aligned}$$

The risk is minimized by f^*. However, f^* is not a unique minimizer. Any f that agrees with f^* at the point $\{x_i, Y_i\}$ also minimizes this risk.
Now, we will make use of the following vector and shorthand notation. The uppercase Y denotes a random variable, while the lowercase y and x denote deterministic quantities.
Equation:

$$Y = \begin{bmatrix} Y_1 \\ Y_2 \\ \vdots \\ Y_n \end{bmatrix} \quad y = \begin{bmatrix} y_1 \\ y_2 \\ \vdots \\ y_n \end{bmatrix} \quad x = \begin{bmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{bmatrix}$$

Then,
$p_f\left(Y\right) = \prod_{i=1}^{n} p(Y_i|f\left(x_i\right))$ (random)
$p_f\left(y\right) = \prod_{i=1}^{n} p(y_i|f\left(x_i\right))$ (deterministic) .
With this notation, the empirical risk and the true risk can be written as
Equation:

$$\begin{aligned} \widehat{R_n}\left(f\right) &= -\frac{1}{n}\ \log p_f\left(Y\right). \\ R(f) &= -\frac{1}{n} E\left[\log p_f\left(Y\right)\right] \\ &= -\frac{1}{n}\int \log p_f\left(y\right)\cdot p_{f^*}\left(y\right)\mathrm{d}y. \end{aligned}$$

Error Bound

Suppose that we have a pool of candidate functions $\mathscr{F}$, and we want to select a function f from $\mathscr{F}$ using the training data. Our usual approach is to show that the distribution of $\widehat{R_n}\left(f\right)$ concentrates about its mean as n grows. First, we assign a complexity $c(f) > 0$ to each $f \in \mathscr{F}$ so that $\sum 2^{-c(f)} \leq 1$. Then, apply the union bound to get a **uniform** concentration inequality holding for all models in $\mathscr{F}$. Finally, we use this concentration inequality to bound the expected risk of our selected model.

We will essentially accomplish the same result here, but avoid the need for explicit concentration inequalities and instead make use of the information-theoretic bounds.

We would like to select an $f \in \mathscr{F}$ so that the excess risk is small.
Equation:

$$\begin{aligned} 0 &\leq R(f) - R\left(f^*\right) \\ &= \frac{1}{n} E\left[\log p_{f^*}(Y) - \log p_f(Y)\right] \\ &= \frac{1}{n} E\left[\log \frac{p_{f^*}(Y)}{p_f(Y)}\right] \\ &\equiv \frac{1}{n} K\left(p_f, p_{f^*}\right) \end{aligned}$$

where
Equation:

$$K\left(p_f, p_{f^*}\right) = \sum_{i=1}^{n} \underbrace{\left(\int \log \frac{p_{f^*(x_i)}(y_i)}{p_{f(x_i)}(y_i)} \cdot p_{f^*(x_i)}(y_i)\, \mathrm{d}y_i\right)}_{K\left(p_{f(x_i)}, p_{f^*(x_i)}\right)}$$

is again the KL divergence.

Unfortunately, as mentioned before, $K\left(p_f, p_{f^*}\right)$ is not a true distance. So instead we will focus on the expected squared Hellinger distance as our measure of performance. We will get a bound on
Equation:

$$\frac{1}{n} E\left[H^2\left(p_f(Y), p_{f^*}(Y)\right)\right] = \frac{1}{n} \sum_{i=1}^{n} \left(\int \left(\sqrt{p_{f(x_i)}(y_i)} - \sqrt{p_{f^*(x_i)}(y_i)}\right)^2 \mathrm{d}y_i\right).$$

Maximum Complexity-Regularized Likelihood Estimation

Theorem
Li-Barron 2000, Kolaczyk-Nowak 2002

Let $\{x_i, Y_i\}_{i=1}^n$ be a random sample of training data with $\{Y_i\}$ independent,
Equation:

$$Y_i \sim p_{f^*(x_i)}(y_i) \quad , i = 1, ..., n$$

for some unknown function f^*.

Suppose we have a collection of candidate functions $\mathscr{F}$, and complexities $c(f) > 0, f \in \mathscr{F}$, satisfying
Equation:

$$\sum_{f \in \mathscr{F}} 2^{-c(f)} \leq 1.$$

Define the complexity-regularized estimator
Equation:

$$\widehat{f_n} \equiv \arg\min_{f \in \mathscr{F}} \left\{ -\frac{1}{n} \sum_{i=1}^{n} \log\ p_f(Y_i) + \frac{2c(f)\,\log 2}{n} \right\}.$$

Then,
Equation:

$$\begin{aligned}\frac{1}{n}E\left[H^2\left(p_f\left(Y\right),p_{f^*}\left(Y\right)\right)\right] &\leq -\frac{2}{n}E\left[\log\left(A\left(p_f\left(Y\right),p_{f^*}\left(Y\right)\right)\right)\right] \\ &\leq \min_{f\in\mathscr{F}}\left\{\frac{1}{n}K\left(p_f,p_{f^*}\right)+\frac{2c(f)\log 2}{n}\right\}.\end{aligned}$$

Before proving the theorem, let's look at a special case.

Example:
Gaussian noise
Suppose $Y_i=f\left(x_i\right)+W_i\quad,W_i\overset{i.i.d.}{\sim}\mathcal{N}\left(0,\sigma^2\right)$.
Equation:

$$p_{f(x_i)}\left(y_i\right)=\frac{1}{\sqrt{2\pi\sigma^2}}e^{-\frac{\left(y_i-f(x_i)\right)^2}{2\sigma^2}}.$$

Using results from example 1, we have
Equation:

$$\begin{aligned}-2\log A\left(p_{\widehat{f_n}}\left(Y\right),p_{f^*}\left(Y\right)\right) &= \sum_{i=1}^{n}-2\log A\left(p_{\widehat{f_n}(x_i)}\left(Y_i\right),p_{f^*(x_i)}\left(Y_i\right)\right) \\ &= \sum_{i=1}^{n}-2\log\int\sqrt{p_{\widehat{f_n}(x_i)}\left(y_i\right)\cdot p_{f^*(x_i)}\left(y_i\right)}\,\mathrm{d}y_i \\ &= \frac{1}{4\sigma^2}\sum_{i=1}^{n}\left(\widehat{f_n}\left(x_i\right)-f^*\left(x_i\right)\right)^2.\end{aligned}$$

Then,
Equation:

$$-\frac{2}{n}E\left[\log\ A\left(p_{\widehat{f_n}},p_{f^*}\right)\right]=\frac{1}{4\sigma^2 n}\sum_{i=1}^{n}E\left[\left(\widehat{f_n}\left(x_i\right)-f^*\left(x_i\right)\right)^2\right].$$

We also have,
Equation:

$$\begin{aligned}\frac{1}{n}K\left(p_f,p_{f^*}\right) &= \frac{1}{n}\sum_{i=1}^{n}\frac{\left(f\left(x_i\right)-f^*\left(x_i\right)\right)^2}{2\sigma^2} \\ -\log\ p_f\left(Y\right) &= \sum_{i=1}^{n}\frac{\left(Y_i-f\left(X_i\right)\right)^2}{2\sigma^2}.\end{aligned}$$

Combine everything together to get
Equation:

$$\widehat{f_n}=\operatorname*{argmin}_{f\in\mathscr{F}}\left\{\frac{1}{n}\sum_{i=1}^{n}\frac{\left(Y_i-f\left(X_i\right)\right)^2}{2\sigma^2}+\frac{2c(f)\log 2}{n}\right\}.$$

The theorem tells us that
Equation:

$$\frac{1}{4n}\sum_{i=1}^{n} E\left[\frac{\left(\widehat{f_n}\left(x_i\right)-f^*\left(x_i\right)\right)^2}{\sigma^2}\right] \leq \min_{f\in\mathscr{F}}\left\{\frac{1}{n}\sum_{i=1}^{n}\frac{\left(f\left(x_i\right)-f^*\left(x_i\right)\right)^2}{2\sigma^2}+\frac{2c(f)\log 2}{n}\right\}$$

or
Equation:

$$\frac{1}{n}\sum_{i=1}^{n} E\left[\left(\widehat{f_n}\left(x_i\right)-f^*\left(x_i\right)\right)^2\right] \leq \min_{f\in\mathscr{F}}\left\{\frac{2}{n}\sum_{i=1}^{n}\left(f\left(x_i\right)-f^*\left(x_i\right)\right)^2+\frac{8\sigma^2 c\left(f\right)\log 2}{n}\right\}.$$

Now let's come back to the proof.
Proof
Equation:

$$\begin{aligned} H^2\left(p_{\widehat{f_n}},p_{f^*}\right) &= \int\left(\sqrt{p_{\widehat{f_n}}\left(y\right)}-\sqrt{p_{f^*}\left(y\right)}\right)^2\mathrm{d}y \\ &\leq -2\log\underbrace{\left(\int\sqrt{p_{\widehat{f_n}}\left(y\right)\cdot p_{f^*}\left(y\right)}\,\mathrm{d}y\right)}_{affinity} \end{aligned}$$

Equation:

$$\Rightarrow$$

Equation:

$$E\left[H^2\left(p_{\widehat{f_n}},p_{f^*}\right)\right] \leq 2\,E\left[\log\left(\frac{1}{\int\sqrt{p_{\widehat{f_n}}\left(y\right)\cdot p_{f^*}\left(y\right)}\,\mathrm{d}y}\right)\right].$$

Now, define the theoretical analog of $\widehat{f_n}$:
Equation:

$$f_n = \operatorname*{argmin}_{f\in\mathscr{F}}\left\{\frac{1}{n}K\left(p_f,p_{f^*}\right)+\frac{2c(f)\log 2}{n}\right\}.$$

Since
Equation:

$$
\begin{aligned}
\widehat{f_n} &= \underset{f\in\mathscr{F}}{\operatorname{argmin}} \left\{ -\frac{1}{n}\,\log p_f\left(Y\right) + \frac{2c(f)\,\log\,2}{n} \right\} \\
&= \underset{f\in\mathscr{F}}{\operatorname{argmax}} \left\{ \frac{1}{n}(\log p_f\left(Y\right) - 2c\left(f\right)\,\log\,2) \right\} \\
&= \underset{f\in\mathscr{F}}{\operatorname{argmax}} \left\{ \frac{1}{2}(\log p_f\left(Y\right) - 2c\left(f\right)\,\log\,2) \right\} \\
&= \underset{f\in\mathscr{F}}{\operatorname{argmax}} \left\{ \log\left(\sqrt{p_f\left(Y\right)} \cdot e^{-c(f)\log 2} \right) \right\} \\
&= \underset{f\in\mathscr{F}}{\operatorname{argmax}} \left\{ \sqrt{p_f\left(Y\right)} \cdot e^{-c(f)\log 2} \right\}
\end{aligned}
$$

we can see that
Equation:

$$
\frac{\sqrt{p_{\widehat{f_n}}\left(Y\right)} e^{-c\left(\widehat{f_n}\right)\log 2}}{\sqrt{p_{f_n}\left(Y\right)} e^{-c(f_n)\log 2}} \geq 1\,.
$$

Then can write
Equation:

$$
\begin{aligned}
E\left[H^2\left(p_{\widehat{f_n}}, p_{f^*}\right)\right] &\leq 2\,E\left[\log\left(\frac{1}{\int \sqrt{p_{\widehat{f_n}}\left(y\right) \cdot p_{f^*}\left(y\right)}\,\mathrm{d}y}\right)\right] \\
&\leq 2\,E\left[\log\left(\frac{\sqrt{p_{\widehat{f_n}}\left(Y\right)} e^{-c\left(\widehat{f_n}\right)\log 2}}{\sqrt{p_{f_n}\left(Y\right)} e^{-c(f_n)\log 2}} \cdot \frac{1}{\int \sqrt{p_{\widehat{f_n}} \cdot p_{f^*}}\,\mathrm{d}y}\right)\right].
\end{aligned}
$$

Now, simply multiply the argument inside the log by $\sqrt{\frac{p_{f^*}(Y)}{p_{f^*}(Y)}}$ to get
Equation:

$$
\begin{aligned}
E\left[H^2\left(p_{\widehat{f_n}}, p_{f^*}\right)\right] &\leq 2\,E\left[\log\left(\frac{\sqrt{p_{f^*}\left(Y\right)}}{\sqrt{p_{f_n}\left(Y\right)}} \frac{\sqrt{p_{\widehat{f_n}}\left(Y\right)}}{\sqrt{p_{f^*}\left(Y\right)}} \frac{e^{-c\left(\widehat{f_n}\right)\log 2}}{e^{-c(f_n)\log 2}} \cdot \frac{1}{\int \sqrt{p_{\widehat{f_n}}\left(y\right) \cdot p_{f^*}\left(y\right)}\,\mathrm{d}y}\right)\right] \\
&= E\left[\log\left(\frac{p_{f^*}\left(Y\right)}{p_{f_n}\left(Y\right)}\right)\right] + 2c\left(f_n\right)\,\log\,2 \\
&\quad +2E\left[\log\left(\frac{\sqrt{p_{\widehat{f_n}}\left(Y\right)}}{\sqrt{p_{f^*}\left(Y\right)}} \cdot \frac{e^{-c\left(\widehat{f_n}\right)\log 2}}{\int \sqrt{p_{\widehat{f_n}}\left(y\right) \cdot p_{f^*}\left(y\right)}\,\mathrm{d}y}\right)\right] \\
&= K\left(p_{f_n}, p_{f^*}\right) + 2c\left(f_n\right)\,\log\,2 \\
&\quad +2E\left[\log\left(\frac{\sqrt{p_{\widehat{f_n}}\left(Y\right)}}{\sqrt{p_{f^*}\left(Y\right)}} \cdot \frac{e^{-c\left(\widehat{f_n}\right)\log 2}}{\int \sqrt{p_{\widehat{f_n}}\left(y\right) \cdot p_{f^*}\left(y\right)}\,\mathrm{d}y}\right)\right].
\end{aligned}
$$

The terms $K\left(p_{f_n}, p_{f^*}\right) + 2c\left(f_n\right) \log 2$ are precisely what we wanted for the upper bound of the theorem. So, to finish the proof we only need to show that the last term is non-positive. Applying Jensen's inequality, we get
Equation:

$$2E\left[\log\left(\frac{\sqrt{p_{\widehat{f_n}}\left(Y\right)}}{\sqrt{p_{f^*}\left(Y\right)}} \cdot \frac{e^{-c\left(\widehat{f_n}\right)\log 2}}{\int \sqrt{p_{\widehat{f_n}}\left(y\right) \cdot p_{f^*}\left(y\right)}\,\mathrm{d}y}\right)\right] \leq 2\log\left(E\left[e^{-c\left(\widehat{f_n}\right)\log 2} \cdot \frac{\sqrt{\frac{p_{\widehat{f_n}}(Y)}{p_{f^*}(Y)}}}{\int \sqrt{p_{\widehat{f_n}}\left(y\right) \cdot p_{f^*}\left(y\right)}\,\mathrm{d}y}\right]\right).$$

Both Y and $\widehat{f_n}$ are random, which makes the expectation difficult to compute. However, we can simplify the problem using the union bound, which eliminates the dependence on $\widehat{f_n}$:
Equation:

$$\begin{aligned}
2E\left[\log\left(\frac{\sqrt{p_{\widehat{f_n}}\left(Y\right)}}{\sqrt{p_{f^*}\left(Y\right)}} \cdot \frac{e^{-c\left(\widehat{f_n}\right)\log 2}}{\int \sqrt{p_{\widehat{f_n}}\left(y\right) \cdot p_{f^*}\left(y\right)}\,\mathrm{d}y}\right)\right] &\leq 2\log\left(E\left[\sum_{f\in\mathscr{F}} e^{-c(f)\log 2} \cdot \frac{\sqrt{\frac{p_f(Y)}{p_{f^*}(Y)}}}{\int \sqrt{p_f\left(y\right) \cdot p_{f^*}\left(y\right)}\,\mathrm{d}y}\right]\right) \\
&= 2\log\left(\sum_{f\in\mathscr{F}} 2^{-c(f)} \frac{E\left[\sqrt{\frac{p_f(Y)}{p_{f^*}(Y)}}\right]}{\int \sqrt{p_f\left(y\right) \cdot p_{f^*}\left(y\right)}\,\mathrm{d}y}\right) \\
&= 2\log\left(\sum_{f\in\mathscr{F}} 2^{-c(f)}\right) \\
&\leq 0.
\end{aligned}$$

where the last two lines come from
Equation:

$$E\left[\sqrt{\frac{p_f\left(Y\right)}{p_{f^*}\left(Y\right)}}\right] = \int \sqrt{\frac{p_f\left(y\right)}{p_{f^*}\left(y\right)}} \cdot p_{f^*}\left(y\right)\mathrm{d}y = \int \sqrt{p_f\left(y\right) \cdot p_{f^*}\left(y\right)}\,\mathrm{d}y$$

and
Equation:

$$\sum_{f\in\mathscr{F}} 2^{-c(f)} \leq 1.$$

Denoising II: Adapting to Unknown Smoothness

Review: Denoising in Smooth Function Spaces I - Method of Sieves

Suppose we make noisy measurements of a smooth function:
Equation:

$$Y_i = f^*(x_i) + W_i, \;\; i = \{1, ..., n\},$$

where
Equation:

$$W_i \overset{i.i.d.}{\sim} N\left(0, \sigma^2\right)$$

and
Equation:

$$x_i = \left(\frac{i}{n}\right).$$

The unknown function f^* is a map
Equation:

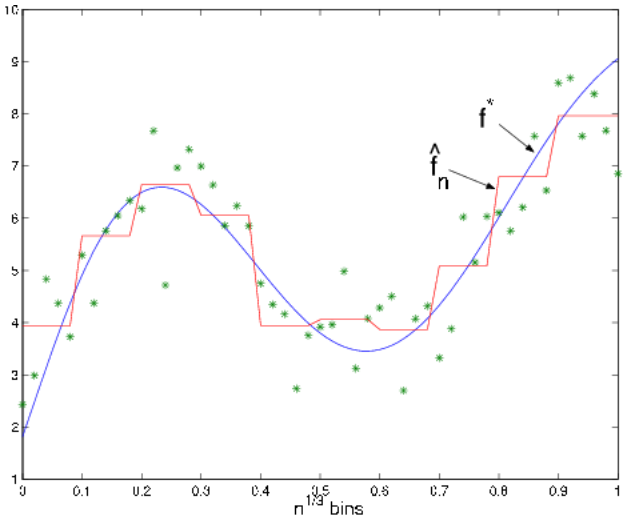
$$f^* : [0, 1] \to \mathbf{R}.$$

In Lecture 4, we consider this problem in the case where f^* was Lipschitz on $[0, 1]$. That is, f^* satisfied
Equation:

$$\left|f^*(t) - f^*(s)\right| \leq L|t - s|, \quad \forall t, s \in [0, 1]$$

where $L > 0$ is a constant. In that case, we showed that by using a piecewise constant function on a partition of $n^{\frac{1}{3}}$ equal-size bins [link] we were able to obtain an estimator $\widehat{f}_n$ whose mean square error was
Equation:

$$E\left[\| f^* - \widehat{f}_n \|^2\right] = O\left(n^{-\frac{2}{3}}\right).$$



Example of the piecewise constant approximation of f^*

In this lecture we will use the Maximum Complexity-Regularized Likelihood Estimation result we derived in Lecture 14 to extend our denoising scheme in several important ways.

To begin with let's consider a broader class of functions.

Hölder Spaces

For $0 < \alpha < 1$, define the space of functions
Equation:

$$H^{\alpha}\left(C_{\alpha}\right) = \left\{ |f| < C_{\alpha} : \sup_{x,h} \frac{|f(x+h) - f(x)|}{|h|^{\alpha}} \leq C_{\alpha} \right\}$$

for some constant $C_{\alpha} < \infty$ and where $f \in L_{\infty}$.H^{α} above contains functions that are bounded, but less smooth than Lipschitz functions. Indeed, the space of Lipschitz functions can be defined as H^1 $(\alpha = 1)$
Equation:

$$H^{1}\left(C_{1}\right) = \left\{ |f| < C_{1} : \sup_{x,h} \frac{|f(x+h) - f(x)|}{|h|} \leq C_{1} \right\}$$

for $C_1 < \infty$. Functions in H^1 are continuous, but those in $H^{\alpha}, \alpha < 1$, are not in general.

Let's also consider functions that are smoother than Lipschitz. If $\alpha = 1 + \beta$, where $0 < \beta < 1$, then define
Equation:

$$H^{\alpha}\left(C_{\alpha}\right) = \left\{ f \in H^{1}\left(C_{\alpha}\right) : \frac{\partial f}{\partial x} \in H^{\beta}\left(C_{\alpha}\right) \right\}.$$

In other words, $H^{\alpha}, 1 < \alpha < 2$, contains Lipschitz functions that are also differentiable and their derivatives are Hölder smooth with smoothness $\beta = \alpha - 1$.

And finally, let
Equation:

$$H^{2}\left(C_{2}\right) = \left\{ f : \frac{\partial f}{\partial x} \in H^{1}\left(C_{2}\right) \right\}$$

contain functions that have continuous derivatives, but that are not necessarily twice-differentiable.

If $f \in H^{\alpha}\left(C_{\alpha}\right)$, $0 < \alpha \leq 2$, then we say that f is Hölder$-\alpha$ smooth with Hölder constant C_{α}. The notion of Hölder smoothness can also be extended to $\alpha > 2$ in a straightforward way.

Note: If $\alpha_{1} < \alpha_{2}$ then
Equation:

$$f \in H^{\alpha_{2}} \Rightarrow f \in H^{\alpha_{1}}.$$

Summarizing, we can describe Hölder spaces as follows. If $f^{*} \in H^{\alpha}(C_{\alpha})$ for some $0 < \alpha \leq 2$ and $C_{\alpha} < \infty$, then

- **(i)**$0 < \alpha \leq 1$ $\quad\quad\quad\quad$ $\left| f^{*}\left(t\right) - f^{*}\left(s\right)\right| \leq C_{\alpha}|t-s|^{\alpha}$
- **(ii)**$1 < \alpha \leq 2$ $\quad\quad\quad\quad$ $\left| \frac{\partial f^{*}}{\partial x}(t) - \frac{\partial f^{*}}{\partial x}(s)\right| \leq C_{\alpha}|t-s|^{\alpha-1}$

Note that in general there is a natural relationship between the Hölder space containing the function and the approximation class used to estimate the function. Here we will consider functions which are Hölder$-\alpha$ smooth where $0 < \alpha \leq 2$ and work with piecewise linear approximations. If we were to consider smoother functions, $\alpha > 2$ we would need consider higher order approximation functions, i.e. quadratic, cubic, etc.

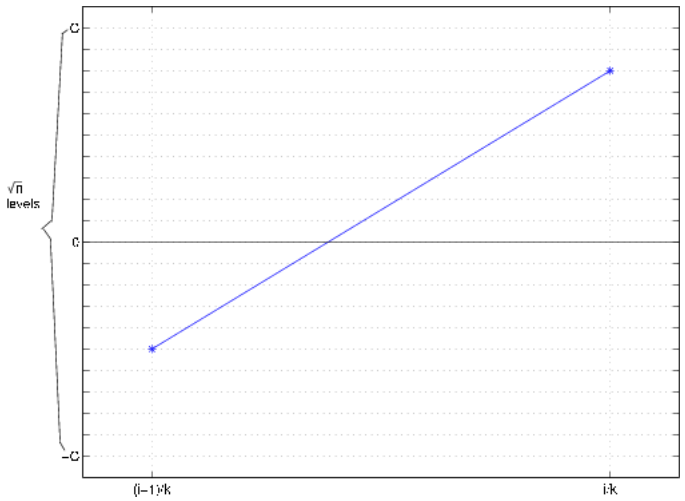
Denoising Example for Signal-plus-Gaussian Noise Observation Model

Now let's assume $f^{*} \in H^{\alpha}\left(C_{\alpha}\right)$ for some unknown $\alpha (0 < \alpha \leq 2)$; i.e. we don't know how smooth f^{*} is. We will use our observations
Equation:

$$Y_{i} = f^{*}\left(x_{i}\right) + W_{i}, \;\; i = \{1, ..., n\},$$

to construct an estimator $\widehat{f}_{n}$. Intuitively, the smoother f^{*} is, the better we should be able to estimate it. Can we take advantage of extra smoothness in f^{*} if we don't know how smooth it is? The smoother f^{*} is, the more averaging we can perform to reduce noise. In other words for smoother f^{*} we should average over larger bins. Also, we will need to exploit the extra smoothness in our approximation of f^{*}. To that end, we will consider candidate functions that are piecewise linear functions on uniform partitions of $[0, 1]$. Let
Equation:

$$\mathscr{F}_{k} = \left\{ |f| \leq C : \begin{array}{l} f \; is \; piecewise \; linear \; on \; \left[0, \frac{1}{k}\right), \left[\frac{1}{k}, \frac{2}{k}\right), ... \left[\frac{k-1}{k}, 1\right) \; and \; the \\ coefficients \; of \; each \; line \; segment \; are \; quantized \; to \frac{1}{2}\log n \; bits. \end{array} \right\}.$$



Example on the quantization of f on interval $\left[\frac{i-1}{k}, \frac{i}{k}\right)$

The start and end points of each line segment are each one of $\sqrt{n}$ discrete values, as indicated in [link]. Since each line may start at any of the $\sqrt{n}$ levels and terminate at any of the $\sqrt{n}$ levels, there are a total of n possible lines for each segment.

Given that there are k intervals we have
Equation:

$$|\mathscr{F}_k| = n^k \Rightarrow \log |\mathscr{F}_k| = k \log n.$$

Therefore we can use $k \log n$ bits to describe a function $f \in \mathscr{F}_k$.

Let
Equation:

$$\mathscr{F} = \bigcup_{k \geq 1} \mathscr{F}_k.$$

Construct a prefix code for every $f \in \mathscr{F}$ by
Equation:

(i) Use $\underbrace{000\cdots1}_{k\,bits}$ to encode the smallest k such that $f \in \mathscr{F}_k$

(ii) Use $k \log n$ bits to encode which element of $\mathscr{F}_k$ we are considering.

Thus, if $f \in \mathscr{F}_k$, then the prefix code associated with f has codeword length
Equation:

$$c(f) = k + k \log n = k(1 + \log n)$$

which satisfies the Kraft Inequality
Equation:

$$\sum_{f \in \mathscr{F}} 2^{-c(f)} \leq 1.$$

Now we will apply our complexity regularization result to select a function $\widehat{f}_n$ from $\mathscr{F}$ and bound its risk. We are assuming Gaussian errors, so
Equation:

$$-\log p_f\left(Y_i\right) = \frac{\left(Y_i - f\left(\frac{i}{n}\right)\right)^2}{2\sigma^2} + constant.$$

We can ignore the constant term and so our empirical selection is
Equation:

$$\widehat{f}_n = \underset{f \in \mathscr{F}}{\operatorname{argmin}} \left\{ \frac{1}{n} \sum_{i=1}^{n} \frac{\left(Y_i - f\left(\frac{i}{n}\right)\right)^2}{2\sigma^2} + \frac{2c(f)\log 2}{n} \right\}.$$

We can compute $\widehat{f}_n$ according to:

For $k = 1, ..., n$
Equation:

$$\widehat{f}_n^{(k)} = \underset{f \in \mathscr{F}_k}{\operatorname{argmin}}\, \widehat{R}_n\left(f\right) = \underset{f \in \mathscr{F}_k}{\operatorname{argmin}}\, \frac{1}{n} \sum_{i=1}^{n} \frac{\left(Y_i - f\left(\frac{i}{n}\right)\right)^2}{2\sigma^2}$$

then select
Equation:

$$\widehat{k} = \underset{k=1,\ldots,n}{\arg\min} \left\{ \widehat{R_n}\left(\widehat{f}_n^{(k)}\right) + \frac{2k(1+\log n)\log 2}{n} \right\}$$

and finally
Equation:

$$\widehat{f}_n = \widehat{f}_n^{\left(\widehat{k}\right)}.$$

Because the KL divergence and -2 log **affinity** simply reduce to squared error in the Gaussian case (Lecture 14), we arrive at a relatively simple bound on the mean square error of $\widehat{f}_n$
Equation:

$$\frac{1}{n}\sum_{i=1}^{n} E\left[\left(\widehat{f}_n\left(\frac{i}{n}\right) - f^*\left(\frac{i}{n}\right)\right)^2\right] \leq \min_{f \in \mathscr{F}} \left\{ \frac{2}{n}\sum_{i=1}^{n}\left(f\left(\frac{i}{n}\right) - f^*\left(\frac{i}{n}\right)\right)^2 + \frac{8\sigma^2 c\left(f\right)\log 2}{n} \right\}.$$

The first term in the brackets above is related to the error incurred by approximating f^* by an element of $\mathscr{F}$. The second term is related to the estimation error involved with the model selection process.

Let's focus on the approximation error. First, suppose $f^* \in H^\alpha(C_\alpha)$ for $1 < \alpha \leq 2$. Let f_k^* be the "best" piecewise linear approximation to f^*, with k pieces on intervals $\left[0, \frac{1}{k}\right), \left[\frac{1}{k}, \frac{2}{k}\right), ... \left[\frac{k-1}{k}, 1\right)$. Consider the difference between f^* and f_k^* on one such interval, say $\left[\frac{i-1}{k}, \frac{i}{k}\right)$. By applying Taylor's theorem with remainder we have

Equation:

$$f^*(t) = f^*\left(\frac{i}{k}\right) + \frac{\partial f^*}{\partial x}(t')\left(t - \frac{i}{k}\right)$$

for $t \in \left[\frac{i-1}{k}, \frac{i}{k}\right)$ and some $t' \in \left[t, \frac{i}{k}\right]$. Define

Equation:

$$f_k^*(t) \equiv f^*\left(\frac{i}{k}\right) + \frac{\partial f^*}{\partial x}\left(\frac{i}{k}\right)\left(t - \frac{i}{k}\right).$$

Note that $f_k^*(t)$ is not necessarily the best piecewise linear approximation to f^*, just good enough for our purposes. Then using the fact that $f^* \in H^\alpha(C_\alpha)$, for $t \in [i - 1/k, i/k)$ we have

Equation:

$$\begin{aligned}
\left|f^*(t) - f_k^*(t)\right| &= \left|\frac{\partial f^*}{\partial x}(t')\left(t - \frac{i}{k}\right) - \frac{\partial f^*}{\partial x}\left(\frac{i}{k}\right)\left(t - \frac{i}{k}\right)\right| \\
&\leq \frac{1}{k}\left|\frac{\partial f^*}{\partial x}(t') - \frac{\partial f^*}{\partial x}\left(\frac{i}{k}\right)\right| \\
&\leq \frac{1}{k} C_\alpha \left|t' - \frac{i}{k}\right|^{\alpha - 1} \\
&\leq \frac{1}{k} C_\alpha \left(\frac{1}{k}\right)^{\alpha - 1} = C_\alpha k^{-\alpha}.
\end{aligned}$$

So, for all $t \in [0, 1]$

Equation:

$$\left|f^*(t) - f_k^*(t)\right| \leq C_\alpha k^{-\alpha}.$$

Now let f_k be the element of $\mathscr{F}_k$ closest to f_k^* (f_k is the quantized version of f_k^*)

Equation:

$$\begin{aligned}
\left|f^*(t) - f_k(t)\right| &= \left|f^*(t) - f_k^*(t) + f_k^*(t) - f_k(t)\right| \\
&\leq \left|f^*(t) - f_k^*(t)\right| + \left|f_k^*(t) - f_k(t)\right| \\
&\leq C_\alpha k^{-\alpha} + \frac{1}{\sqrt{n}}
\end{aligned}$$

since we used $\frac{1}{2}\log n$ bits to quantize the endpoints of each line segment. Consequently,

Equation:

$$\begin{aligned}\left|f^{*}(t)-f_{k}^{*}(t)\right|^{2} &\leq \left|f^{*}(t)-f_{k}^{*}(t)\right|^{2}+2\left|f^{*}(t)-f_{k}^{*}(t)\right|\left|f_{k}^{*}(t)-f_{k}(t)\right|+\left|f_{k}^{*}(t)-f_{k}(t)\right|^{2} \\ &\leq C_{\alpha}^{2}k^{-2\alpha}+2C_{\alpha}\frac{k^{-\alpha}}{\sqrt{n}}+\frac{1}{n}.\end{aligned}$$

Thus it follows that
Equation:

$$\min_{f\in\mathscr{F}_{k}}\left\{\frac{2}{n}\sum_{i=1}^{n}\left(f(i/n)-f^{*}(i/n)\right)^{2}+\frac{8\sigma^{2}c(f)\log 2}{n}\right\}\leq 2C_{\alpha}^{2}k^{-2\alpha}+\frac{4C_{\alpha}k^{-\alpha}}{\sqrt{n}}+\frac{2}{n}+\frac{8\sigma^{2}k(\log n+1)\,\mathrm{lc}}{n}$$

The first and last terms dominate the above expression. Therefore, the upper bound is minimized when $k^{-2\alpha}$ and $\frac{k}{n}$ are balanced. This is accomplished by choosing $k=\left\lfloor n^{\frac{1}{2\alpha+1}}\right\rfloor$. Then it follows that
Equation:

$$\min_{f\in\mathscr{F}_{k}}\left\{\frac{2}{n}\sum_{i=1}^{n}\left(f\left(\frac{i}{n}\right)-f^{*}\left(\frac{i}{n}\right)\right)^{2}+\frac{8\sigma^{2}c(f)\log 2}{n}\right\}=O\left(n^{-\frac{2\alpha}{2\alpha+1}}\log n\right).$$

If $\alpha=2$ then we have
Equation:

$$\frac{1}{n}\sum_{i=1}^{n}E\left[\left(\widehat{f}_{n}\left(\frac{i}{n}\right)-f^{*}\left(\frac{i}{n}\right)\right)^{2}\right]=O\left(n^{-\frac{4}{5}}\log n\right).$$

If $f^{*}\in H^{\alpha}(C_{\alpha})$ for $0<\alpha\leq 1$, let f_{k}^{*} be the following piecewise constant approximation to f^{*}. Let
Equation:

$$f_{k}^{*}(t)\equiv f^{*}\left(\frac{i}{n}\right)\text{ on interval }\left[\frac{i-1}{k},\frac{i}{k}\right).$$

Then
Equation:

$$\begin{aligned}\left|f^{*}(t)-f_{k}^{*}(t)\right| &= \left|f^{*}(t)-f^{*}\left(\frac{i}{n}\right)\right| \\ &\leq C_{\alpha}\left|t-\frac{i}{n}\right|^{\alpha} \\ &\leq C_{\alpha}k^{-\alpha}.\end{aligned}$$

Repeating the same reasoning as in the $1<\alpha\leq 2$ case, we arrive at
Equation:

$$\frac{1}{n}\sum_{i=1}^{n}E\left[\left(\widehat{f}_{n}\left(\frac{i}{n}\right)-f^{*}\left(\frac{i}{n}\right)\right)^{2}\right]=O\left(n^{-\frac{2\alpha}{2\alpha+1}}\log n\right)$$

for $0<\alpha\leq 1$. In particular, for $\alpha=1$ we get

Equation:

$$\frac{1}{n}\sum_{i=1}^{n} E\left[\left(\widehat{f}_n\left(\frac{i}{n}\right) - f^*\left(\frac{i}{n}\right)\right)^2\right] = O\left(n^{-\frac{2}{3}}\log n\right)$$

within a logarithmic factor of the rate we had before (in Lecture 4) for that case!

Summary

1. $\widehat{f}_n$ can be computed by finding least-square line fits to the data on partitions of the form $\left[0, \frac{1}{k}\right), \left[\frac{1}{k}, \frac{2}{k}\right), ... \left[\frac{k-1}{k}, 1\right)$ for $k = 1, ..., n$, and then selecting the best fit by the $\widehat{k}$ that gives the minimum of the complexity regularization criterion.
2. If $f^* \in H^\alpha(C_\alpha)$ for some $0 < \alpha \leq 2$, then
   Equation:
$$MSE\left(\widehat{f}_n\right) = \frac{1}{n}\sum_{i=1}^{n} E\left[\left(\widehat{f}_n\left(\frac{i}{n}\right) - f^*\left(\frac{i}{n}\right)\right)^2\right] = O\left(n^{-\frac{2\alpha}{2\alpha+1}}\log n\right).$$
3. $\widehat{f}_n$ automatically picks the optimal number of bins. Essentially $\widehat{f}_n$ (indirectly) estimates the smoothness of f^* and produces a rate which is near minimax optimal ! ($n^{-\frac{2\alpha}{2\alpha+1}}$ is the best possible).
4. The larger α is the faster the convergence and the better the denoising !

Nonlinear Approximation and Wavelet Analysis

Review

In Lecture 4 and 15, we investigated the problem of denoising a smooth signal in additive white noise. In Lecture 4, we considered Lipschitz functions and showed that by filling constants on a uniform partition of width $n^{-1/3}$ we can achieve an $n^{-2/3}$ rate of MSE convergence.

In Lecture 15, we considered Holder-α smooth functions, and we demonstrated that by automatically selecting partition width and using polynomial fits we can obtain a MSE convergence rate of $n^{-2\alpha/2\alpha+1}$, substantially better when $\alpha > 1$. Also important is the fact that we don't need to know the value of α a priori. The estimator $\widehat{f}_n$ is fundamentally different than its counterpart in Lecture 4.

In both cases $\widehat{f}_n(t)$ is a linear function (polynomial on constant fit) of the data in each interval of the underlying partition. In Lecture 4, the partition was independent of the data, and so the overall estimator is a linear function of the data .

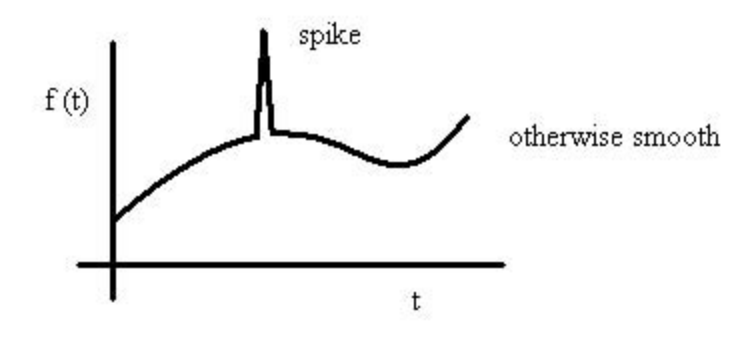
However, in Lecture 15 the partition itself was selected based on the data. Consequently, $\widehat{f}_n(t)$ is a non-linear function of the data . Linear estimators (linear functions of the data) cannot adapt to unknown degrees of smoothness. In this lecture, we lay the groundwork for one more important extension in the denoising application - spatial adaptivity. That is, we would like to construct estimators that not only adapt to unknown degrees of global smoothness, but that also adapt to spatially varying degrees of smoothness.

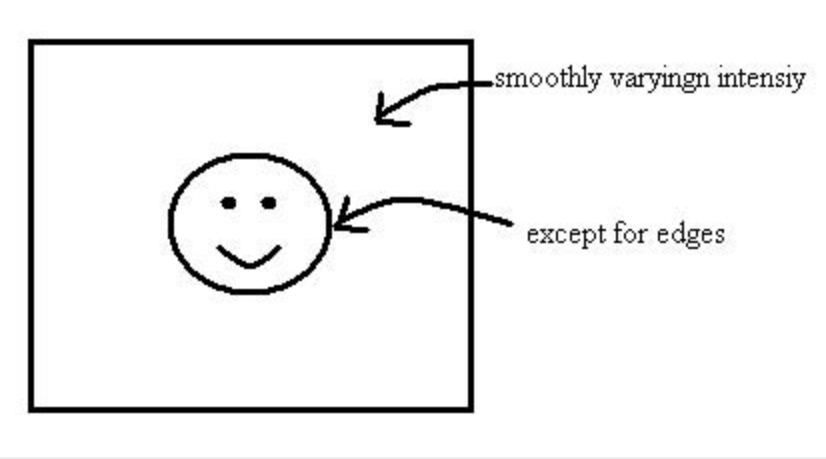
We will focus on the approximation theoretic aspects of the problem in this lecture, considering tree-based approximations and wavelet expansions. In the next lecture, we will apply these results to the denoising problem, this will bring us up to date with the current state-of-the-art in denoising and non-parametric estimation.

Recall that Holder spaces contain smooth functions that are well approximated with polynomials or piecewise polynomial functions. Holder spaces are quite large and contain many interesting signals. However, Holder spaces are still inadequate in many applications. Often, we encounter functions that are not smooth everywhere; they contain discontinuities, jumps, spikes, etc. Indeed, the "singularities" (or non-smooth points) can be the most interesting and informative aspects of the functions.

Example:
Functions not smooth everywhere.

Example of functions not smooth everywhere. (a) 1-D Case (b) 2-D Case

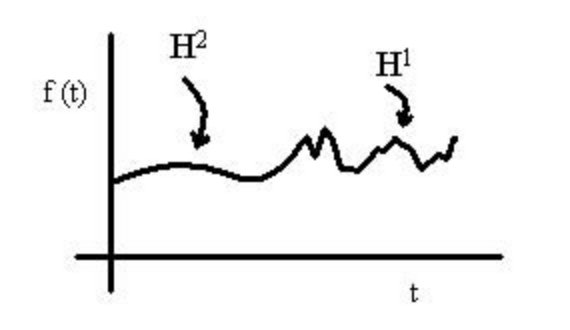


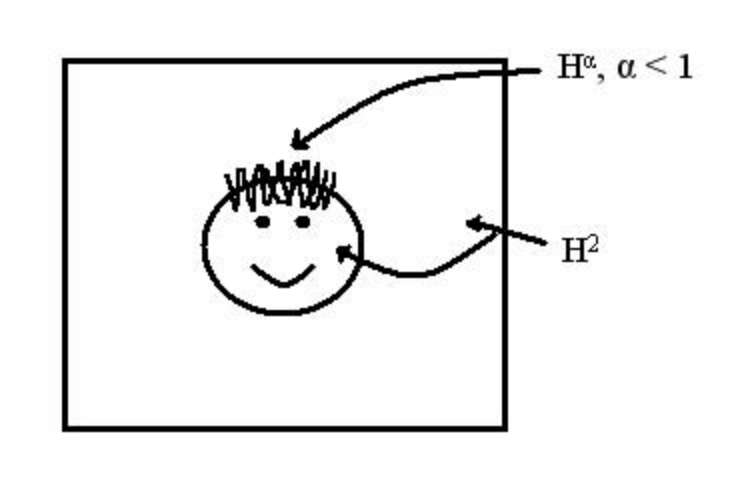


Furthermore, functions of interest may possess different degrees of smoothness in different regions.

Example:
Functions with different degrees of smoothness.

Example of functions having different degrees of smoothness. (a) 1-D Case (b) 2-D Case





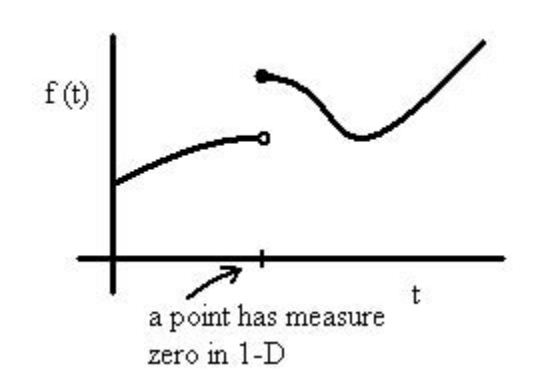
NonLinear Approximation via Trees

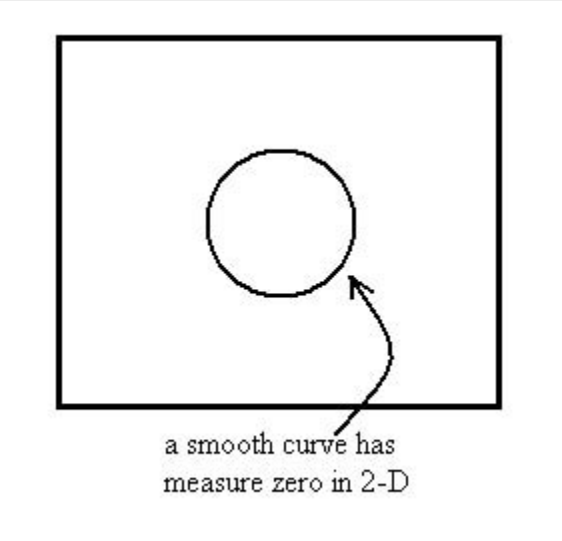
Let $B^{\alpha}\left(C_{\alpha}\right)$ denote the set of all functions that are $H^{\alpha}\left(C_{\alpha}\right)$ everywhere except on a set of measure zero. To simplify the notation, we won't explicitly identify the domain (e.g., $[0,1]$ or $[0,1]^{d}$); that will be clear from the context.

Example:

Sets of measure zero

Sets of measure zero. (a) 1-D Case (b) 2-D Case



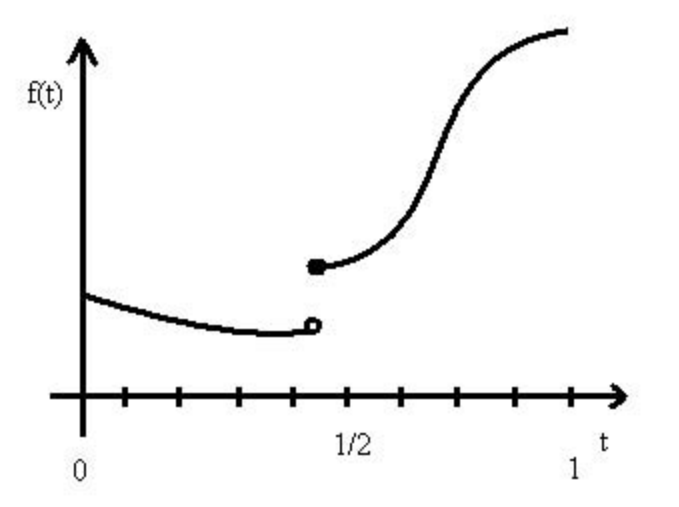


Let's consider a 1-D case first.
Let $f \in B^{\alpha}\left(C_{\alpha}\right)$ and consider approximating f by a piecewise polynomial function on a uniform partition.
If f is Holder-α smooth everywhere, then by using an appropriate partition width k^{-1} and fitting degree $\lceil \alpha \rceil$ polynomials on each interval we have an approximation f_k satisfying
Equation:

$$\left|f\left(t\right)-f_k\left(t\right)\right| \leq C_{\alpha} k^{-\alpha}$$

and
Equation:

$$||f - f_k||_{L_2}^2 = O\left(k^{-2\alpha}\right).$$



Smooth curve with a discontinuity.

However, if there is a discontinuity then for t in the interval containing the discontinuity the difference

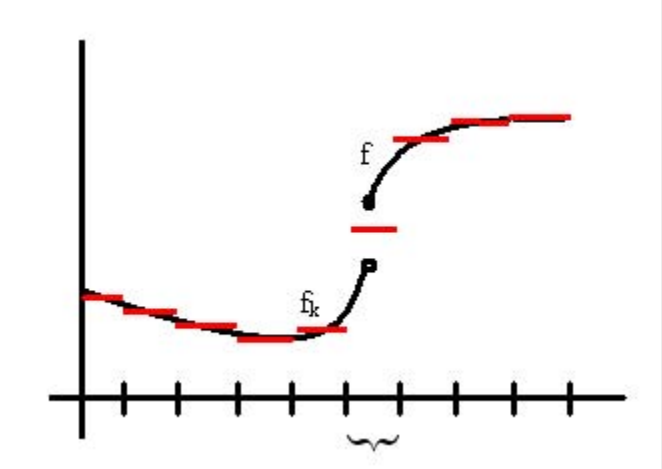
Equation:

$$|f(t) - f_k(t)|$$

will not be small.

Example:

Suppose f is piecewise Lipschitz and f_k ia a piecewise constant.



Equation:

$$|f(t) - f_k(t)| \approx \Delta$$

where Δ is a constant equal to average of f on right and left side of discontinuity in this interval.

Equation:

$$\Rightarrow ||f - f_k||_{L_2}^2 = O\left(k^{-1}\right)$$

where k^{-1} is the width of the interval. Notice this rate is quite slow. This problem naturally suggests the following remedy: use very small intervals near discontinuities and larger intervals in smooth regions. Specifically, suppose we use intervals of width $k^{-2\alpha}$ to contain the discontinuities and the intervals of width k^{-1} elsewhere. Then accordingly piecewise polynomial approximation $\widetilde{f}_k$ satisfies

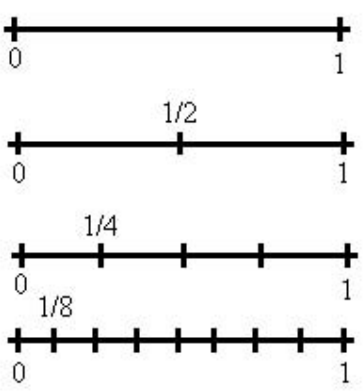
Equation:

$$||f - \widetilde{f}_k||_{L_2}^2 = O\left(k^{-2\alpha}\right).$$

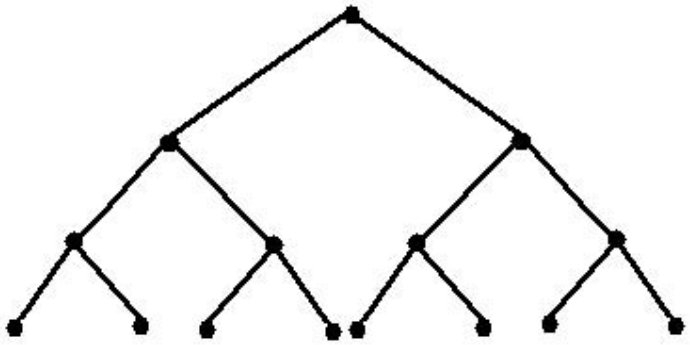
We can accomplish this need for "adaptive resolution" or "multiresolution" using recursive partitions and trees.

Recursive Dyadic Partitions

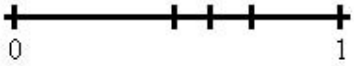
We discussed this idea already in our examination of classification trees. Here is the basic idea again, graphically.



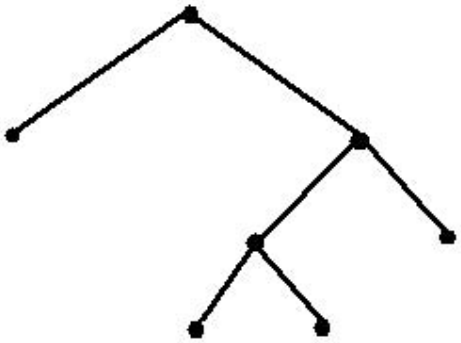
complete RDP



corresponding tree



pruned RDP



corresponding tree

Complete and pruned RDP along with their correspnding tree structures.

Consider a function $f \in B^{\alpha}(C_{\alpha})$ that contains no more than m points of discontinuity, and is $H^{\alpha}(C_{\alpha})$ away from these points.

Lemma

Consider a complete RDP with n intervals, then there exists an associated pruned RDP with $O(klogn)$ intervals, such that an associated piecewise degree $\lceil \alpha \rceil$ polynomial approximation $\tilde{(}f)_k$, has a squared approximation error of $O\big(min\left(k^{-2\alpha}, n^{-1}\right)\big)$.

Assume $n > k > m$. Divide $[0, 1]$ into k intervals. If f is smooth on a particular interval I, then
Equation:

$$|f\left(t\right) - \widetilde{f}_k\left(t\right)| = O\left(k^{-2\alpha}\right) \forall t \in I.$$

In intervals that contain a discontinuity, recursively subdivide into two until the discontinuity is contained in an interval of width n^{-1}. This process results in at most $log_2 n$ addition subintervals per discontinuity, and the squared approximation error is $O(k - 2\alpha)$ on all of them accept the m intervals of width n^{-1} containing the discontinuities where the error is $O(1)$ at each point.

Thus, the overall squared L_2 norm is
Equation:

$$||f - \widetilde{f}_k||_{L_2}^2 = O\left(min\left(k^{-2\alpha}, n^{-1}\right)\right)$$

and there are at most $k + log_2 n$ intervals in the partition. Since k>m, we can upperbound the number of intervals by $2klog_2 n$.

Note that if the initial complete RDP has $n \approx k^{2\alpha}$ intervals, then the squared error is $O\big(k^{-2\alpha}\big)$.

Thus, we only incur a factor of $2\alpha logk$ additional leafs and achieve the same overall approximation error as in the $H^{\alpha}\left(C_{\alpha}\right)$ case. We will see that this is a small price to pay in order to handle not only smooth functions, but also piecewise smooth functions.

Wavelet Approximations

Let $f \in L^2([0,1]); \int f^2(t)dt < \infty$.

A wavelet approximation is a series of the form
Equation:

$$f = c_o + \sum_{j \geq 0} \sum_{k=1}^{2^j} < f, \psi_{j,k} > \psi_{j,k}$$

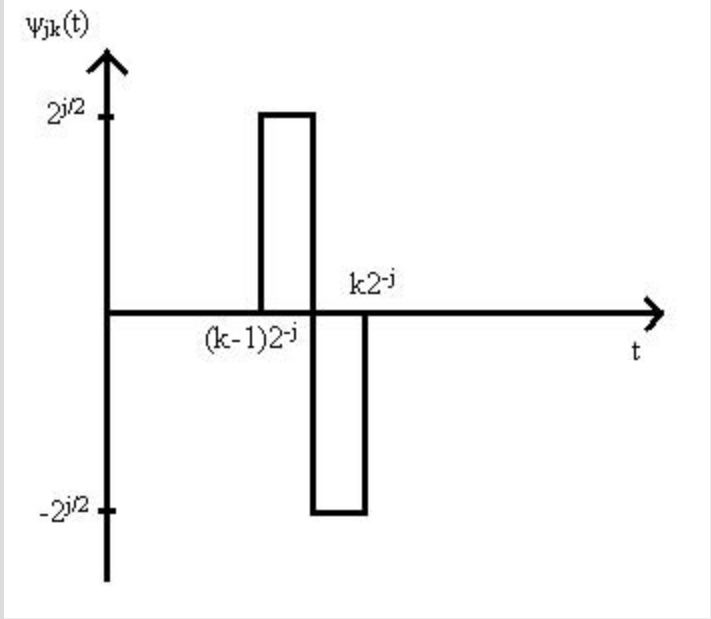
where c_o is a constant $\left(c_o = \int_0^1 f(t)dt\right)$,
Equation:

$$< f, \psi_{j,k} >= \int_0^1 f(t)\psi_{j,k}(t)dt$$

and the basis functions $\psi_{j,k}$ are orthonormal, oscillatory signals, each with an associated scale 2^{-j} and position $k2^{-j}$. $\psi_{j,k}$ is called the wavelet at scale 2^{-j} and position $k2^{-j}$.

Example:
Haar Wavelets
Equation:

$$\psi_{j,k}(t) = 2^{j/2}\left(\mathbf{1}_{\{t \in [2^{-j}(k-1), 2^{-j}(k-1/2)]\}} - \mathbf{1}_{\{t \in [2^{-j}(k-1/2), 2^{-j}k]\}}\right)$$



Haar Wavelet

Equation:

$$\int_0^1 \psi_{j,k}(t)dt = 0$$

Equation:

$$\int_0^1 \psi_{j,k}^2(t)dt = \int_{(k-1)2^{-j}}^{k2^{-j}} 2^j dt = 1$$

Equation:

$$\int_0^1 \psi_{j,k}(t)\psi_{l,m}(t)dt = \delta_{j,l}.\,\delta_{k,m}$$

Note: If f is constant on $\left[2^{-j}(k-1), 2^{-j}k\right]$, then

Equation:

$$\int f\psi_{j,k}\left(t\right)=0.$$

Suppose f is piecewise constant with at most m discontinuities. Let
Equation:

$$f_J=c_o+\sum_{j=0}^{J-1}\sum_{k=1}^{2^j}<f,\psi_{j,k}>\psi_{j,k}.$$

Then, f_J has at most mJ non-zero wavelet coefficients; i.e.,
$<f,\psi_{j,k}>=0$ for all but mJ terms, since at most one Haar Wavelet at each scale senses each point of discontinuity. Said another way, all but at most m of the wavelets at each scale have support over constant regions of f.
f_J itself will be piecewise constant with discontinuities only possible occurring at end points of the intervals $\left[2^{-J}\left(k-1\right),2^{-J}k\right]$. Therefore, in this case
Equation:

$$||f-f_J||_{L_2}^2=O\left(2^{-J}\right).$$

Daubechies wavelets are the extension of the Haar wavelet idea. Haar wavelets have one "vanishing moment":
Equation:

$$\int_0^1\psi_{j,k}=0.$$

Daubechies wavelets are "smoother" basis functions with extra vanishing moments. The Daubechies-N wavelet has N vanishing moments.
Equation:

$$\int_0^1 t^l\psi_{j,k}dt=0 for l=0,1,\ldots,N-1.$$

The Daubechies-1 wavelet is just the Haar case.
If f is a piecewise degree $\leq N$ polynomial with at most m pieces, then using the Daubechies-N wavelet system.
Equation:

$$||f - f_J||_{L_2}^2 = O\left(2^{-J}\right);$$

and
Equation:

$$f_J(t) = c_o + \sum_{j=0}^{J-1} \sum_{k=1}^{2^j} < f, \psi_{j,k} > \psi_{j,k}(t)$$

has at most $O(mJ)$ non-zero wavelet coefficients. f_J is called the Discrete Wavelet Transform (DWT) approximation of f. The key idea is the same as we saw with trees.

Sampled Data

We can also use DWT's to analyze and represent discrete, sampled functions. Suppose,
Equation:

$$\underline{f} = [f(1/n), f(2/n), \ldots, f(n/n)]$$

then we can write $\underline{f}$ as
Equation:

$$\underline{f} = c_o + \sum_{j=0}^{log_2 n - 1} \sum_{k=1}^{2^j} < \underline{f}, \psi_{j,k} > \psi_{j,k}$$

where

Equation:

$$\psi_{j,k} = [\psi_{j,k}(1), \psi_{j,k}(2), \ldots, \psi_{j,k}(n)]$$

is a discrete time analog of the continuous time wavelets we considered before. In particular,
Equation:

$$\sum_{i=1}^{n} i^l \psi_{j,k}(i) = 0, l = 0, 1, \ldots, N-1$$

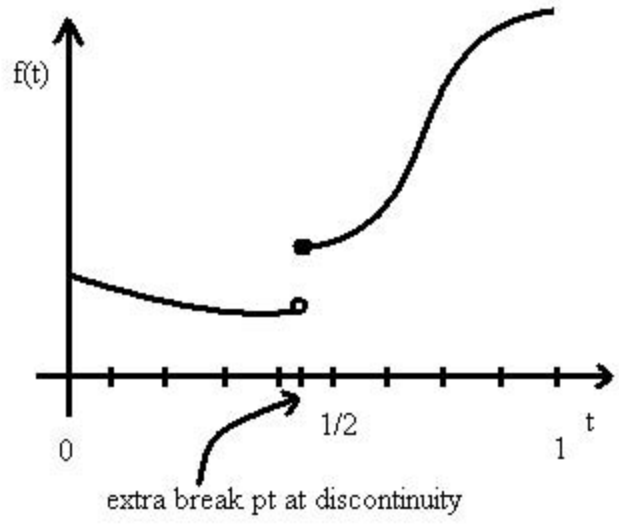
for the Daubechies-N discrete wavelets.
Equation:

$$< \underline{f}, \psi_{j,k} >= \underline{f}^T \psi_{j,k}$$

Thus, we also have an analogous approximation result: If $\underline{f}$ are samples from a piecewise degree $\leq N$ polynomial function with a finite number m of discontinuities, then $\underline{f}$ has $O(mJ)$ non-zero wavelet coefficients.

Approximating functions with wavelets

Suppose $f \in B^{\alpha}(C_{\alpha})$ and has a finite number of discontinuities. Let f_p denote piecewise degree-$N (N = \lceil \alpha \rceil)$ polynomial approximation to f with $O(k)$ pieces; a uniform partition into k equal length intervals followed by addition splits at the points of discontinuity.



Then
Equation:

$$|f(t)-f_p(t)|^2 = O\left(k^{(}-2\alpha\right)\right) \forall t \in [0,1]$$

Equation:

$$\Rightarrow |f(i/n)-f_p(i/n)|^2 = O\left(k^{-2\alpha}\right) i = 1,\ldots,n$$

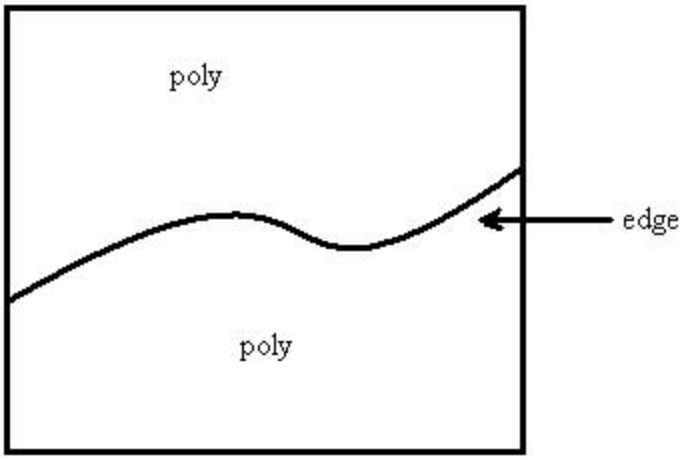
Equation:

$$\Rightarrow 1/n||\underline{f}-\underline{f}_p||_{L_2}^2 = O\left(k^{-2\alpha}\right)\Big)$$

and $\underline{f}_p$ has $O(klog_2 n)$ non-zero coefficients according to our previous analysis.

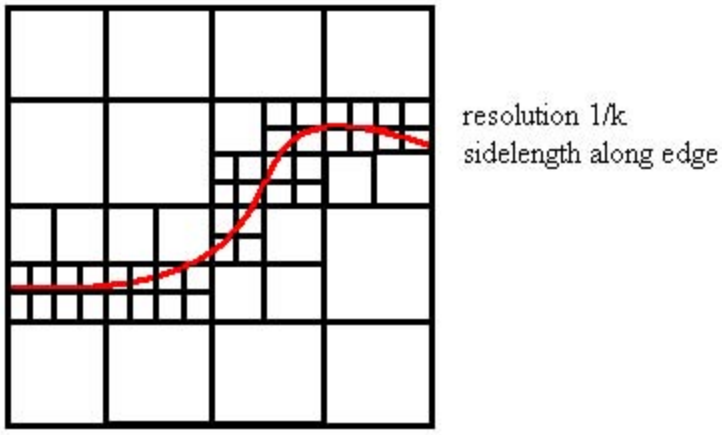
Wavelets in 2-D

Suppose f is a 2-D image that is piecewise polynomial:



A pruned RDP of k squares decorated with polyfits gives
Equation:

$$||f - f_k||_{L_2}^2 = O\left(k^{-1}\right).$$



Let $\underline{f} = [f\,(i/k, j/k)_{i,j=1}^{n}$ sample range.
Equation:

$$f_n(t) = \sum_{i,j=1}^{k} f(i/k, j/kk) \mathbf{1}_{\{t \in [i-1/k, i/k) x [j-1/k, j/k)\}}$$

then
Equation:

$$||f - f_n||_{L_2}^2 = O\left(k^{-1}\right)$$

$O(1)$ error on k of the k^2 pixels, near zero elsewhere. The DWT of $\underline{f}$ has $O(k)$ non-zero wavelet coefficients. $O\left(2^j\right)$ at scale
$2^{-j}, j = 0, 1, \ldots, logn.$

Vapnik-Chervonenkis Theory

Review of Past Lecture

In our past lectures we considered collections of candidate function $\mathscr{F}$ that were either **finite** or **enumerable**. We then constructed penalties, usually codelengths, for each candidate $c(f)$, $f \in \mathscr{F}$, such that $\sum_{f \in \mathscr{F}} 2^{c(f)} \leq 1$ This allowed us to derive uniform concentration inequalities over the entire set $\mathscr{F}$ using the union bound. However, in many cases the collections $\mathscr{F}$ may be uncountably infinite. A simple example is the collection $\mathscr{F}$ of a single threshold classifier in 1-d having the form
Equation:

$$f_t\left(x\right) = \mathbf{1}_{\{x \geq t\}}$$

and their complements
Equation:

$$f_s\left(t\right) = \mathbf{1}_{\{x < s\}}.$$

Thus, $\mathscr{F}$ contains an uncountable number of classifiers, and we cannot apply the union bound argument in such cases.

Two Ways to Proceed

Discretize or Quantize the Collection

Example:
To quantize $\mathscr{F}$
Equation:

$$F_q = \left\{f, f\left(x\right) = \mathbf{1}_{\{x \leq 1/q_i i \in \{0,1,\ldots,q\}\}}\right\}$$

q is positive, such that $\forall f_q \in \mathscr{F}_q$
Equation:

$$\int \left| f - f_q \right| \leq c/q$$

if the density of x is bounded by $c > 0$. $q < n^{1/2}$.

Identical Empirical Errors

Consider the fact that given only n training data, many of the classifiers in such a collection may produce identical empirical errors. Also, many $f \in \mathscr{F}$ will produce identical label assignments on the data. We will have at most 2^n unique labels.

f is uncountable, its interceptions are countable and bounded by 2^n. n intervals with 2 classifier per interval.

The number of distinct labeling assignments that a class $\mathscr{F}$ can produce on a set of n points is denoted
Equation:

$$S\left(\mathscr{F}, n\right) \leq 2^n$$

The VC dimension is $logS(\mathscr{F}, n)$. Specifically, $VC(\mathscr{F}) = k$, where k is largest integer such that $S\left(\mathscr{F}, k\right) = 2^k$ Ex. $2n = 2^n$, $n = 2$, $VC(\mathscr{F}) = 2$.

Ex. Consider
Equation:

$$\mathscr{F} = \left\{ f : f\left(x\right) = \mathbf{1}_{\{x \geq t\}} or f\left(x\right) = \mathbf{1}_{\{x < t\}}, t \in \left[0, 1\right] \right\}$$

Let q be a positive integer and
Equation:

$$\mathscr{F}_q = \left\{ f : f\left(x\right) = \mathbf{1}_{\{x \geq i/q\}} or f\left(x\right) = \mathbf{1}_{\{x < i/q\}}, i \in \left\{0, 1, ..., q\right\} \right\}$$

and,

Equation:

$$|f_q| = 2(q+1).$$

Moreover, for any $f \in \mathscr{F}$ there exists an $f_1 \in \mathscr{F}_q$ such that
Equation:

$$\int \left| f(x) - f_q(x) \right| dx \leq \int_{(i-1)/q}^{i/q} 1 dx = 1/q.$$

Now suppose we have n training data and suppose $f^* \in \mathscr{F}$. We know that in general, the minimum empirical risk classifier will converge to the Bayes classifier at the rate of $n^{-1/2}$ or slower. Therefore, it is unnecessary to drive the approximation error down faster than $n^{-1/2}$ So, we can restrict our attention of $\mathscr{F}_{n^{-1/2}}$ and, provided that the density of x is bound above. We have
Equation:

$$min_{f \in \mathscr{F}_{n^{-1/2}}} R(f) - R\left(f^*\right) \leq C_{f_q} min \int \left| f^*(x) - f(x) \right| dx \leq c/n^{1/2}.$$

Vapnik-Chervonenkis theory is based not on explicitly quantizing the collection of candidate functions, but rather on recognizing that the richness of $\mathscr{F}$ is limited in a certain sense by the number of training data. Indeed, given n i.i.d. training data, there are at most 2^n different binary labelings. Therefore, any collection $\mathscr{F}$ may be divided into 2^n subsets of classifiers that are "equilvalent" with respect to the training data. In many cases a collection may not even be capable of producing 2^n different labellings.

Example

Consider $X = [0,1]$.
Equation:

$$\mathscr{F} = \left\{ f : f(x) = \mathbf{1}_{\{x \geq t\}} or f(x) = \mathbf{1}_{\{x < t\}} t \in [0,1] \right\}$$

Suppose we have n training data: $(x_1, ..., x_n) \in [0,1]$. With x^s denotes the location of each training point in [0,1]. Associated with each x is a label $y \in \{0,1\}$. Any classifier in $\mathscr{F}$ will label all points to the left of a number $t \in [0,1]$ as "1" or "0", and points to the right as "0" or "1", respectively. For $t \in [0, x_1)$, all points are either labelled "0" or "1". For $t \in (x_1, x_2)$, x_1 is labelled "0" or "1" and $x_2 ... x_n$ are label "1" or "0" and so on. We see that there are exactly $2n$ different labellings; far less than 2^n!

The number of different labellings that a class $\mathscr{F}$ can produce on a set of n training data is a measure of the "effective size" of $\mathscr{F}$. The Vapnik-Chervonenkis (VC) dimension of $\mathscr{F}$ is proportional to the log of the effective size. Let $V(\mathscr{F}, n)$ denote the VC dimension of $\mathscr{F}$, typically a constant, independent of n. The VC inequality states that for all $f \in \mathscr{F}$
Equation:

$$P\left(\left|\widehat{R}_n(f) - R(f)\right| > \epsilon\right) \leq 8e^{V(\mathscr{F},h)}e^{-n\epsilon^2/32}.$$

This type of uniform concentration inequality can be used in a similar fashion to our use of Hoeffding's inequality plus union bound.

Hyperplane Classifiers

We will go into the details of VC Theory next lecture, and the remainder of this lecture will introduce the key ideas with an example Consider the following setup. Let $X = [0,1]^d$, $Y = \{0,1\}$ Let
Equation:

$$\mathscr{F} = \left\{f : f(x) = \mathbf{1}_{\{w^T x + w_0 > 0\}}\right\}$$

with w_0 and $w \in R^{d+1}$ This is the collection of all hyperplane classifiers. $\mathscr{F}$ is infinite and uncountable.

Suppose that we have n training data
Equation:

$$\{X_i, Y_i\}_{i=1}^n.$$

There are at most $2\binom{n}{d}$ unique classifiers in $\mathscr{F}$ with respect to these data. To see this, consider d arbitrary data points $x_1, ..., x_{i_d}$, and let $w^T x + w_0 > 0$ be a hyperplane containing these points. To be specific, take the hyperplane with
Equation:

$$||w_0 w|| = 1.$$

this hyperplane coincides with two possible classification rules:
Equation:

$$f_1(x) = \mathbf{1}_{\{w^T x + w_0 > 0\}}$$

Equation:

$$f_2(x) = \mathbf{1}_{\{w^T x + w_0 < 0\}}$$

Each d-tuple of training data produces two distinct classifiers, assuming the data are not co-linear. Thus, there are at most $2*\binom{n}{d}$ unique classifiers in $\mathscr{F}$ with respect to the training data. (All other $f \in \mathscr{F}$ produce the same labels and empirical risk as one of the classifiers.) Let's enumerate the unique hyperplane classifiers $f_1, ..., f_{2*\binom{n}{d}}$, and let
Equation:

$$\widehat{f}_n = \text{arg} \min_{f \in \{f_1, ..., f_2\binom{n}{d}\}} \widehat{R}_n(f)$$

and let
Equation:

$$R^* = inf_{f \in \mathscr{F}} R(f)$$

and define
Equation:

$$f^* = argmin_{f \in \mathscr{F}} R(f)$$

If multiple $f \in \mathscr{F}$ achieve R^*, pick f^* to be one of them in an arbitrary fixed number.

Theorem

Assume that P_x has a density, but that the distribution of (x, y) is other arbitrary. If $n \geq d$ and $2d/n \leq \epsilon \leq 1$ then

Equation:

$$P\left(R\left(\widehat{f}_n\right) - R\left(f\right) > \epsilon\right) \leq e^{2d\epsilon}\left(2\binom{n}{d} + 1\right)e^{-n\epsilon^2/2}.$$

Note: The assumption that P_x has a density insures that no d+1 points are co-planar. This in turn, guarantees that there are exactly $2\binom{n}{d}$ unique classifier and that the $2\binom{n}{d}$ under consideration are fully representative of all possible classifiers in $\mathscr{F}$, with respect to the data.

The proof is a specialization of the basic ingredients of VC Theory to the case at hand. Here we follow the proof in DGL '96. First we note that,

Equation:

$$R\left(\widehat{f}_n\right) - R\left(f^*\right) = R\left(\widehat{f}_n\right) - \widehat{R}_n\left(\widehat{f}_n\right) + \widehat{R}_n\left(\widehat{f}_n\right) - R\left(f^*\right)$$

Equation:

$$\leq R\left(\widehat{f}_n\right) - \widehat{R}_n\left(\widehat{f}_n\right) + \widehat{R}_n f^*) - R\left(f^*\right) + d/n$$

and since $\widehat{R}_n\left(\widehat{f}_n\right) \leq \widehat{R}_n\left(f\right) + d/n$ for any $f \in \mathscr{F}$

Equation:

$$\leq max_{i=1,\ldots,2\binom{n}{d}}(R\left(f_i\right) - \hat{(}R)_n\left(f_i\right)) + \hat{(}R)_n\left(f^*\right) - R\left(f^*\right) + d/n.$$

Therefore, by the union bound:
Equation:

$$P\left(R\left(\widehat{f}_n\right) - R\left(f^*\right) > \epsilon\right)$$

Equation:

$$\leq \sum_{i=1}^{2\binom{n}{d}} P\Big(R\left(f_i\right) - \widehat{R}_n\left(f_i\right) > \epsilon/2\Big) + P\Big(\widehat{R}_n\left(f^*\right) - R\left(f^*\right) + d/n > \epsilon/2\Big).$$

We can bound the second term of the above bound using Chernoff's/Hoeffding's inequality:
Equation:

$$P\Big(\widehat{R}_n\left(f^*\right) - R\left(f^*\right) > \epsilon/2 - d/n\Big)$$

Equation:

$$\leq e^{-2n(\epsilon/2 - d/n)^2}$$

Equation:

$$\leq e^{2d\epsilon} e^{-n\epsilon^2/2}.$$

Next, let's bound one of the terms in the summation. For example, take
Equation:

$$P\Big(R\left(f_i\right) - \widehat{R}_n\left(f_i\right) > (\epsilon/2)\Big).$$

Note that by symmetry all $2\binom{n}{d}$ terms will have identical bounds. Since the bounds are independent of $P_x y$.

Assume that f_1 is determined by the first d data points $x_14, ..., x_d$. By the smoothing property of expectations we can write,
Equation:

$$P\Big(R\left(f_i\right) - \widehat{R}_n\left(f\right) > \epsilon/2\Big) = E\Big[P\Big(R\left(f_i\right) - \widehat{R}_n\left(f_i\right) > \epsilon/2|x_1, ..., x_d\Big)\Big].$$

From here, we will bound the conditional probability inside the expectation. Let $(X_1'', Y_1''), ..., \left(X_d'', Y_d''\right)$ be d additional random samples that are independent and identically distributed as the data $(X_1, Y_1), ..., (X_d, Y_d)$. $\{X_i'', Y_i''\}_{i=1}^d$ are often called the "ghost sample" since they are not actually observed. They are a fictious sample leads to a simple bound on the conditional probability. Define if $i \leq d$
Equation:

$$\left(X_i^{'}, Y_i^{'}\right) = \left(X_i'', Y_i''\right)$$

or if $i > d$
Equation:

$$\left(X_i^{'}, Y_i^{'}\right) = (X_i, Y_i).$$

That is, $\left\{X_i^{'}, Y_i^{'}\right\}_{i=1}^d$ agrees with our observed data on i>d, but the first d samples are replaced with the ghost sample. Then,
Equation:

$$P\Big(R\left(f_i\right) - \widehat{R}_n\left(f_1\right) > \epsilon/2|x_1, ..., x_d\Big)$$

Equation:

$$\leq P\left(R\left(f_i\right) - 1/n\sum_{i=d+1}^{n} 1_{f_1(x_i) \neq y_i} > \epsilon/2|x_1, ..., x_d\right)$$

Equation:

$$\leq P\left(R\left(f_i\right)-1/n\sum_{1}^{n}1_{f_1(x_i)\neq y_i}+d/n>\epsilon/2|x_1,...,x_d\right)$$

Equation:

$$=P\Big(R\left(f_i\right)-\hat{\Big(}R\big)_n^{'}\left(f_1\right)>t/2-d/n|x_1,...,x_d\Big)$$

where,
Equation:

$$\widehat{R}_n^{'}\left(f_1\right)=1/n\sum_{i=1}^{n}\mathbf{1}_{\left\{f_1\left(x_i^{'}\right)\neq y_i^{'}\right\}}.$$

Note that $n\hat{\Big(}R\big)_n^{'}\left(f_1\right)$ is binomially distributed with mean $R(f_1)$ and it is independent of $x_1,...,x_d$ Therefore,
Equation:

$$P\Big(R\left(f_i\right)-\widehat{R}_n^{'}\left(f_1\right)>\epsilon/2-d/n|x_1,...,x_d\Big)$$

Equation:

$$=P\Big(R\left(f_i\right)-\widehat{R}_n^{'}\left(f_1\right)>t/2-d/n\Big|x_1,...,x_d\Big)$$

Equation:

$$\leq e^{-2n(\epsilon/2-d/n)^2}$$

Equation:

$$\leq e^{2d\epsilon}e^{-n\epsilon^2/2}.$$

In conclusion,
Equation:

$$P\Big(R\left(\widehat{f}_n\right) - R^* > \epsilon\Big)$$

Equation:

$$\leq \sum_{i=1}^{2\binom{n}{d}} P\Big(R(f)_i - \widehat{R}_n\left(t_i\right) > \epsilon/2\Big) + P\Big(\widehat{R}_n\left(f^*\right) - R\left(f^*\right) + d/n > \epsilon/2\Big)$$

Equation:

$$\leq 2\binom{n}{d} e^{2d\epsilon} e^{-n\epsilon^2/2} + e^{2d\epsilon} e^{-n\epsilon^2/2}$$

Equation:

$$= e^{2d\epsilon}\Big(2\binom{n}{d} + 1\Big) e^{-n\epsilon^2/2}.$$

Lastly, Corollary If $n \geq d$, then
Equation:

$$E\Big[R\left(\widehat{f}_n\right) - min_{f \in \mathscr{F}} R\left(f\right)\Big] \leq \sqrt{2(d+1)(logn+2)/n}.$$

The Vapnik-Chervonenkis Inequality

The Vapnik-Chervonenkis Inequality

The VC inequality is a powerful generalization of the bounds we obtained for the hyperplane classifier in the previous lecture. The basic idea of the proof is quite similar. Before starting the inequality, we need to introduce the concept of shatter coefficients and VC dimension .

Shatter Coefficients

Let $\mathscr{A}$ be a collection of subsets of $\mathscr{R}^d$, definition : The n^{th} shatter coefficient of $\mathscr{A}$ is defined by
Equation:

$$\mathscr{S}_{\mathscr{A}}(n) = \max_{x_1, ..., x_n \epsilon \mathscr{R}^d} \left| \left\{ \{x_1, ..., x_n\} \bigcap A, A \epsilon \mathscr{A} \right\} \right|.$$

The shatter coefficients are a measure of the richness of the collection $\mathscr{A}$. $\mathscr{S}_{\mathscr{A}}(n)$ is the largest number of different subsets of a set of n points that can be generated by intersecting the set with elements of $\mathscr{A}$.

Example:
In 1-d, Let $\mathscr{A} = \{(-\infty, t], t \epsilon \mathscr{R}\}$ Possible subsets of $\{x_1, ..., x_n\}$ generated by intersecting with sets of the form $(-\infty, t]$ are
$\{x_1, ..., x_n\}$, $\{x_1, ..., x_{n-1}\}$, ..., $\{x_1\}$, φ. Hence $\mathscr{S}_d(n) = n + 1$.

Example:
In 2-d, Let $\mathscr{A}$ = { all rectangles in $\mathscr{R}^2$}
Consider a set $\{x_1, x_2, x_3, x_4\}$ of training points. If we arrange the four points into the corner of a diamond shape. It's easy to see that we can find a rectangle in $\mathscr{R}^2$ to cover any subsets of the four points as the above picture, i.e. $\mathscr{S}_{\mathscr{A}}(4) = 2^4 = 16$.
Clearly, $\mathscr{S}_{\mathscr{A}}(n) = 2^n, n = 1, 2, 3$ as well.
However, for $n = 5, \mathscr{S}_{\mathscr{A}}(n) < 2^5$. This is because we can always select four points such that the rectangle, which just contains four of them, contains the other

point. Consequently, we cannot find a rectangle classifier which contains the four outer points and does not contain the inner point as shown above.
Note the $\mathscr{S}_{\mathscr{A}} \leq 2^n$.
If $|\{\{x_1, ..., x_n\} \bigcap A, A \, \epsilon \, \mathscr{A}\}| = 2^n$ then we say that $\mathscr{A}$ shatters $x_1, \, ..., \, x_n$.

VC Dimension

The VC dimension
$V_{\mathscr{A}}$ of a collection of sets $\mathscr{A}$ is defined as the largest interger n such that $S_{\mathscr{A}}(n) = 2^n$.

Example:
$\mathscr{A} = \{(-\infty, t] \, ; t \, \epsilon \, \mathscr{R}\}, \mathscr{S}_{\mathscr{A}} = n + 1$ hence $\mathscr{V}_{\mathscr{A}} = 1$.

Example:
$\mathscr{A}$ = { all rectangles in $\mathscr{R}^2$}.
$\mathscr{S}_{\mathscr{A}} = 2^n, n = 1, 2, 3, 4$ and $\mathscr{S}_{\mathscr{A}} \leq 2^n, n = 4$, Hence $V_{\mathscr{A}} = 4$.
The VC dimension provides a useful bound on the growth of the shatter coefficients.

Sauer's Lemma:

Let $\mathscr{A}$ be a collection of set with VC dimension $V_{\mathscr{A}} < \infty$. Then
$\forall n, \mathscr{S}_{\mathscr{A}}(n) \leq \sum_{i=0}^{V_{\mathscr{A}}} \binom{n}{i}$, also $\mathscr{S}_{\mathscr{A}}(n) \leq (n+1)^{V_{\mathscr{A}}}, \forall n$.

VC Dimension and Classifiers

Let $\mathscr{F}$ be a collection of classifiers of the form $f : \mathscr{R}^d \rightarrow \{0, 1\}$ Define
$\mathscr{A} = \{\{x : f(x) = 1\} \times \{0\} \bigcup \{x : f(x) = 0\} \times \{1\}, f \, \epsilon \, \mathscr{F}\}$ In words, this is collection of subsets of $\mathscr{X} \times \mathscr{Y}$ for which on $f \epsilon \mathscr{F}$ maps the features x to a label opposite of y. The size of $\mathscr{A}$ expresses the richness of $\mathscr{F}$. The larger $\mathscr{A}$ is the more likely it is that there exists an $f \epsilon \mathscr{F}$ for which $R(f) = P(f(X) \neq Y)$ is close to the Bayes risk $R^* = P\left(f^*(X) \neq Y\right)$ where f^* is the Bayes classifier. The n^{th} shatter

coefficient of $\mathscr{F}$ is defined as $\mathscr{S}_{\mathscr{F}}(n) = \mathscr{S}_{\mathscr{A}}(n)$ and the VC dimesion of $\mathscr{F}$ is defined as $V_{\mathscr{F}} = V_{\mathscr{A}}$.

Example:
linear (hyperplane) classifiers in $\mathscr{R}^d$
Consider d = 2. Let n be the number of training points, it is easy to see that when $n = 1$, let $\mathscr{A}$ be as above. By using linear classifiers in $\mathscr{R}^2$, it is easy to see that we can assign 1 to all possible subsets $\{\{x_1\}, \varphi\}$ and 0 to their complements. Hence $\mathscr{S}_{\mathscr{F}}(1) = 2$.
When $n = 2$, we can also assign 1 to all possible subsets $\{\{x_1, x_2\}, \{x_1\}, \{x_2\}, \varphi\}$ and 0 to their complements, and vice versa. Hence $\mathscr{S}_{\mathscr{F}}(2) = 4 = 2^2$.
When $n = 3$, we can arrange arrange the point x_1, x_2, x_3(non-colinear) so that the set of linear classifiers shatters the three points, hence $\mathscr{S}_{\mathscr{F}}(3) = 8 = 2^3$
When $n = 4$, no matter where the points x_1, x_2, x_3, x_4 and what designated binary values y_1, y_2, y_3, y_4 are. It's clear that $\mathscr{A}$ does not shatter the four points. To see the claim, first observe that the four points will form a 4-gon (if the four points are co-linear, or if the three points are co-linear then clearly linear classifiers cannot shatter the points). The two points that belong to the same diagonal lines form 2 groups and no linear classifier can assign different values to the 2 groups. Hence $\mathscr{S}_{\mathscr{F}}(4) < 16 = 2^4$ and $V_{\mathscr{F}} = 3$.
We state here without proving it that in general the class of linear classifiers in $\mathscr{R}^d$ has $V_{\mathscr{F}} = d + 1$.

The VC Inequality

Let X_1, , ..., X_n be i.i.d. $\mathscr{R}^d$-valued random variables. Denote the common distribution of $X_i, 1 \leq i \leq n$ by $\mu(A) = P(X_1 \epsilon A)$ for any subset $A \subset \mathscr{R}^d$. Similarly, define the empirical distribution $\mu_n(A) = \frac{1}{n}\sum_1^n 1_{\{X_i \epsilon A\}}$.

Theorem
VC '71

For any probablilty measure μ and collection of subsets $\mathscr{A}$, and for any $\epsilon > 0$.
Equation:

$$P\left(\sup_{A \epsilon \mathscr{A}} |\mu_n(A) - \mu(A)| > \epsilon\right) \leq 8\mathscr{S}_{\mathscr{A}}(n) e^{-n\epsilon^2/32}$$

and
Equation:

$$E\left[\underset{A\epsilon\mathscr{A}}{sup}|\mu_n\left(A\right)-\mu\left(A\right)|\right]\leq 2\sqrt{\frac{\log 2\mathscr{S}_{\mathscr{A}}\left(n\right)}{n}}$$

Before giving a proof to the theorem. We present a Corollary.
Corollary

Let $\mathscr{F}$ be a collection of classifiers of the form $f:\mathscr{R}^d\rightarrow\{0,1\}$ with VC dimension $V_{\mathscr{F}}<\infty,$ Let $R(f)=P(f(X)\neq Y)$ and $\widehat{R}_n\left(f\right)=\frac{1}{n}\sum_1^n 1_{\{f(X_i)\neq Y_i\}}$, where $X_i,Y_i,1\leq i\leq n$ are i.i.d. with joint distribution P_{XY}.

Define

$$\widehat{f}_n=\underset{f\epsilon\mathscr{F}}{argmin}\,\widehat{R}_n\left(f\right).$$

Then
Equation:

$$E\left[R\left(\widehat{f}_n\right)\right]-\underset{f\epsilon\mathscr{F}}{inf}R\left(f\right)\leq 4\sqrt{\frac{\mathscr{V}_{\mathscr{F}}\log\left(n+1\right)+\log 2}{n}}.$$

Let $\mathscr{A}=\{\{x:f(x)=1\}\times\{0\}\bigcup\{x:f(x)=0\}\times\{1\},f\,\epsilon\,\mathscr{F}\}$

Note that
Equation:

$$P(f(X)\neq Y)=P((X,Y)\,\epsilon\,A):=\mu(A)$$

where $A=\{x:f(x)=1\}\times\{0\}\bigcup\{x:f(x)=0\}\times\{1\}.$

Similarly,
Equation:

$$\frac{1}{n}\sum_{1}^{n}1_{\{f(X_i)\neq Y_i\}}=\frac{1}{n}\sum_{1}^{n}1_{\{(X_i,Y_i)\,\epsilon\,A\}}:=\mu\left(A\right).$$

Therefore, according to the VC theorem.
Equation:

$$\begin{aligned}E\left[\underset{f\,\epsilon\,\mathscr{F}}{sup}\left|\widehat{R}_n\left(f\right)-R\left(f\right)\right|\right]=E\left[\underset{A\,\epsilon\,\mathscr{A}}{sup}\left|\mu_n\left(A\right)-\mu\left(A\right)\right|\right] &\leq 2\sqrt{\frac{\log 2\mathscr{S}_{\mathscr{A}}\left(n\right)}{n}}\\ &= 2\sqrt{\frac{\log 2\mathscr{S}_{\mathscr{F}}\left(n\right)}{n}}\end{aligned}$$

Since $V_{\mathscr{F}}<\infty,\mathscr{S}_{\mathscr{F}}\left(n\right)\leq\left(n+1\right)^{V_{\mathscr{F}}}$ and
Equation:

$$E\left[\underset{f\epsilon\mathscr{F}}{sup}\left|\widehat{R}_n\left(f\right)-R\left(f\right)\right|\right]\leq 2\sqrt{\frac{V_{\mathscr{F}}\log\left(n+1\right)+\log 2}{n}}.$$

Next, note that
Equation:

$$\begin{aligned}R\left(\widehat{f}_n\right)-\underset{f\,\epsilon\,\mathscr{F}}{inf}R\left(f\right) &= \left[R\left(\widehat{f}_n\right)-\widehat{R}_n\left(\widehat{f}_n\right)\right]+\left[\widehat{R}_n\left(\widehat{f}_n\right)-\underset{f\,\epsilon\,\mathscr{F}}{inf}R\left(f\right)\right]\\ &= \left[R\left(\widehat{f}_n\right)-\widehat{R}_n\left(\widehat{f}_n\right)\right]+\left[\underset{f\,\epsilon\,\mathscr{F}}{sup}\left(\widehat{R}_n\left(\widehat{f}_n\right)-R\left(f\right)\right)\right]\\ &\leq \left[R\left(\widehat{f}_n\right)-\widehat{R}_n\left(\widehat{f}_n\right)\right]+\left[\underset{f\,\epsilon\,\mathscr{F}}{sup}\left(\widehat{R}_n\left(f\right)-R\left(f\right)\right)\right]\\ &\leq 2\underset{f\,\epsilon\,\mathscr{F}}{sup}\left|\widehat{R}_n\left(f\right)-R\left(f\right)\right|\end{aligned}.$$

Therefore,
Equation:

$$
\begin{aligned}
E\left[R\left(\widehat{f}_n\right)\right] - \inf_{f \in \mathscr{F}} R(f) &\leq 2E\left[\sup_{f \in \mathscr{F}} \left|\widehat{R}_n(f) - R(f)\right|\right] \\
&\leq 4\sqrt{\frac{V_{\mathscr{F}} \log(n+1) + \log 2}{n}}
\end{aligned}
.
$$

Applications of VC Bound

Linear Classifiers

Suppose $\mathscr{F}$= {linear classifiers in $\mathbf{R}^d$}, then we have
Equation:

$$V_{\mathscr{F}} = d+1, \quad \widehat{f}_n = \operatorname*{argmin}_{f \in \mathscr{F}} \widehat{R}_n(f)$$

Equation:

$$E\left[R\left(\widehat{f}_n\right)\right] - \inf_{f \in \mathscr{F}} R(f) \leq 4\sqrt{\frac{(d+1)\log(n+1) + \log 2}{n}}.$$

Generalized Linear Classifiers

Normally, we have a feature vector $X \in \mathbf{R}^d$. A hyperplane in $\mathbf{R}^d$ provides a linear classifier in $\mathbf{R}^d$. Nonlinear classifiers can be obtained by a straightforward generalization.

Let $\varphi_1, \cdots, \varphi_{d'}$, $d' \geq d$ be a collection of functions mapping $\mathbf{R}^d \to \mathbf{R}$. These functions, applied to a feature $X \in \mathbf{R}^d$, produce a generalized set of features, $\varphi = (\varphi_1(X), \varphi_2(X), \cdots, \varphi_{d'}(X))'$. For example, if $X = (x_1, x_2)'$, then we could consider $d' = S$ and $\varphi = \left(x_1, x_2, x_1 x_2, x_1^2, x_2^2\right)' \in \mathbf{R}^5$. We can then construct a linear classifier in the higher dimensional generalized feature space $\mathbf{R}^{d'}$.

The VC bounds immediately extend to this case, and we have for $\mathscr{F}'$ = { generalized linear classifiers based on maps $\varphi : \mathbf{R}^d \to \mathbf{R}^{d'}$ },
Equation:

$$E\left[R\left(\widehat{f}_n\right)\right] - \inf_{f \in \mathscr{F}'} R(f) \leq 4\sqrt{\frac{(d'+1)\log(n+1) + \log 2}{n}}.$$

Half-Space Classifiers

Theorem
Steele '75, Dudley '78

Let $\mathscr{G}$be a finite-dimensional vector space of real-valued functions on $\mathbf{R}^d$. The class of sets $\mathscr{A} = \{\{x : g(x) \geq 0\} : g \in \mathscr{G}\}$ has VC dimension $\geq$ dim($\mathscr{G}$).

It is sufficient to show that no set of $n = dim(\mathscr{G}) + 1$ points can be shattered by $\mathscr{A}$. Take any n points and for each $g \in \mathscr{G}$, define the vector $V_g = (g(x_1), \cdots, g(x_n))$.

The set $\{V_g : g \in \mathscr{G}\}$ is a linear subspace of $\mathbf{R}^n$ of dimension $\leq$ dim ($\mathscr{G}$) = $n - 1$. Therefore, there exists a non-zero vector $\alpha = (\alpha_1, \cdots, \alpha_n) \in \mathbf{R}^n$ such that $\sum_{i=1}^n \alpha_i g(x_i) = 0$. We can assume that at least one of these α_i^S is negative (if all are positive, just negate the sum). We can then re-arrange this expression as $\sum_{i:\alpha_i \geq 0} \alpha_i g(x_i) = \sum_{i:\alpha_i < 0} -\alpha_i g(x_i)$.

Now suppose that there exists a $g \in \mathscr{G}$ such that the set $\{x : g(x) \geq 0\}$ selects precisely the x_i^S on the left-hand side above. Then all terms on the left are non-negative and all the terms on the right are non-positive. Since α is non-zero, this is a contradiction. Therefore, $x_1, \cdots, x_n$ cannot be shattered by sets in $\{x : g(x) \geq 0\}$, $g \in \mathscr{G}$. 6.375pt0.0pt6.375pt

Example:
Consider half-spaces in $\mathbf{R}^d$ of the form $\mathscr{A} = \left\{x \in \mathbf{R}^d : x_i \geq b, i \in \{1, \cdots, d\}, b \in R\right\}$. Each half-space can be described by
Equation:

$$g(x) = [0, \cdots, 0, 1, 0, \cdots, 0] \begin{bmatrix} x_1 \\ \vdots \\ x_d \end{bmatrix} - b$$

Equation:

$$\Rightarrow dim(\mathscr{G}) = d + 1, \quad V_{\mathscr{A}} \leq d + 1.$$

Tree Classifiers

Let
Equation:

$$\mathscr{T}_k = \{recursive \quad rectangular \quad partitions \quad of \quad \mathbf{R}^d \quad with \quad k+1 \quad cells\}$$

Let $T \in \mathscr{T}_k$. Each cell of T results from splitting a rectangular region into two smaller rectangles parallel to one of the coordinate axes.

Example:
$T \in \mathscr{T}_3$, $d = 2$.
Each additional split is analogous to a half-space set. Therefore, each additional split can potentially shatter $d+1$ points. This implies that
Equation:

$$V_{\mathscr{T}_k} \leq (d+1)k.$$

Example:
$d = 1$.
$k = 1$ split shatters two points.
$k = 2$ splits shatters three points < 4.

VC Bound for Tree Classifiers

Equation:

$$\mathscr{F}_k = \{tree \quad classifiers \quad with \quad k+1 \quad leafs \quad on \quad \mathbf{R}^d\}$$

Equation:

$$E\left[R\left(\widehat{f}_n\right)\right] - \inf_{f \in \mathscr{F}_k} R(f) \leq 4\sqrt{\frac{(d+1)k \log n + \log 2}{n}}.$$

Exercise:

Problem:

How can we decide what dimension to choose for a generalized linear classifier?

How many leafs should be used for a classification tree?

Solution:

Complexity Regularization using VC bounds!

Structural Risk Minimization (SRM)

SRM is simply complexity regularization using VC type bounds in place of Chernoff's bound or other concentration inequalities.

The basic idea is to consider a sequence of sets of classifiers $\mathscr{F}_1, \mathscr{F}_2, ...$, of increasing VC dimensions $V_{\mathscr{F}_1} \leq V_{\mathscr{F}_2} \leq ....$ Then for each $k = 1, 2, ...$ we find the minimum empirical risk classifier
Equation:

$$\widehat{f}_n^{(k)} = \operatorname*{argmin}_{f \in \mathscr{F}_k} \widehat{R}_n(f)$$

and then select the final classifier according to
Equation:

$$\widehat{k} = \operatorname*{argmin}_{k \geq 1} \left\{ \widehat{R}_n\left(\hat{t}_n^{(k)}\right) + \sqrt{\frac{32 V_{\mathscr{F}_k} (\log n + 1)}{n}} \right\}$$

and $\widehat{f}_n \equiv \widehat{f}_n^{\left(\widehat{k}\right)}$ is the final choice.

The basic rational is that we know
Equation:

$$R_n\left(\widehat{f}_n^{(k)}\right) - \inf_{f \in \mathscr{F}_k} R(f) \leq C' \sqrt{\frac{V_{\mathscr{F}_k} \log n}{n}}$$

where C' is a constant.

The end result is that
Equation:

$$E\left[R\left(\widehat{f}_n\right)\right] \leq \min_{k \geq 1} \left\{ \min_{f \in \mathscr{F}_k} R(f) + 16 \sqrt{\frac{V_{\mathscr{F}_k} \log n + 4}{2n}} \right\}$$

analogous to our pervious complexity regularization results, except that codelengths are replaced by VC dimensions.

In order to prove the result we use the VC probability concentration bound and assume that $\triangle = \sum_{k \geq 1} V_{\mathscr{F}_k} < \infty$. This enables a union bounding argument and leads to a risk bound of the form given above.

Key Point of VC Theory

Complexity of classes depends on richness (shattering capability) relative to a set of n arbitrary points. This allows us to effectively “quantize" collections of functions in a slightly data-dependent manner.

Application to Trees

Let
Equation:

$$\mathscr{F}_k = \left\{ k \quad leaf \quad decision \quad trees \quad in \quad \mathbf{R}^d \right\}, \quad V_{\mathscr{F}_k} \leq (d+1)(k+1)$$

Equation:

$$\widehat{f}_n^{(k)} = \arg\min_{f \in \mathscr{F}_k} \widehat{R}_n(f)$$

Equation:

$$\widehat{k} = \underset{k \geq 1}{\operatorname{argmin}} \left(\min_{f \in \mathscr{F}_k} R(f) + \sqrt{\frac{32(d+1)(k-1)(\log n + 1)}{n}} \right)$$

Then
Equation:

$$\widehat{f}_n = \widehat{f}_n^{\left(\widehat{k}\right)}$$

satisfies
Equation:

$$E\left[R\left(\widehat{f}_n\right)\right] \leq \min_{k \geq 1} \left(\min_{f \in \mathscr{F}_k} R(f) + 16\sqrt{\frac{(d+1)(k-1)\log n + 4}{2n}} \right)$$

compare with
Equation:

$$E\left[R\left(\widehat{f}_n\right)\right] \leq \min_{k \geq 1} \left(\min_{f \in dyadic\ k\ leaf\ trees} R(f) + \sqrt{\frac{(3k-1)\log 2 + \frac{1}{2}\log n}{2n}} \right)$$

from Lecture 11.

Lower Performance Bounds for Estimators

Lower Performance Bounds

In other modules, estimators/predictors are analyzed, in order to obtain upper bounds on their performance. These bounds are of the form:
Equation:

$$\min_{f \in \mathscr{F}} \mathbb{E}\left[d\left(\widehat{f}_n, f\right)\right] \leq Cn^{-\gamma}$$

where $\gamma > 0$. We would like to know if these bounds are tight, in the sense that there is no other estimator that is significantly better. To answer this, we need lower bounds like
Equation:

$$\inf_{\widehat{f}_n} \sup_{f \in \mathscr{F}} \mathbb{E}\left[d\left(\widehat{f}_n, f\right)\right] \geq cn^{-\gamma}$$

We assume we have the following ingredients:

- *Class of models, $\mathscr{F} \subseteq \mathscr{S}$. $\mathscr{F}$ is a class of models containing the “true" model and is a subset of some bigger class $\mathscr{S}$. E.g. $\mathscr{F}$ could be the class of Lipschitz density functions or distributions P_{XY} satisfying the box-counting condition.
- *An observation model, $\mathscr{P}_f$, indexed by $f \in \mathscr{F}$. $\mathscr{P}_f$ denotes the distribution of the data under model f. E.g. in regression and classification, this is the distribution of $Z = (X_1, Y_1, \cdots, X_n, Y_n) \subseteq \mathscr{Z}$. We will assume that $\mathscr{P}_f$ is a probability measure on the measurable space $(\mathscr{Z}, \mathscr{B})$.
- *A performance metric $d(.,.) \geq 0$. If you have a model estimate $\widehat{f}_n$, then the performance of that model estimate relative to the true model f is $d\left(\widehat{f}_n, f\right)$. E.g.

  Equation:

$$\text{Regression:} \qquad d\left(\widehat{f}_n, f\right) = ||\widehat{f}_n - f||_2 = \left(\int \left(\widehat{f}_n(x) - f(x)\right)^2 dx\right)^{1/2}$$

  Equation:

$$\text{Classification:} \qquad d\left(\widehat{f}_n, f\right) = R\left(\widehat{G}_n\right) - R^* = \int_{\widehat{G}_n \Delta G^*} |2\eta(x) - 1| dP_X(x)$$

As before, we are interested in the risk of a learning rule, in particular the maximal risk given as:
Equation:

$$\sup_{f \in \mathscr{F}} \mathbb{E}_f\left[d\left(\widehat{f}_n, f\right)\right] = \sup_{f \in \mathscr{F}} \int d\left(\widehat{f}_n(Z), f\right) d\mathscr{P}_f(Z)$$

where $\widehat{f}_n$ is a function of the observations Z and $\mathbb{E}_f$ denotes the expectation with respect to $\mathscr{P}_f$.

The main goal is to get results of the form
Equation:

$$\mathscr{R}_n^* \overset{\Delta}{=} \inf_{\widehat{f}_n} \sup_{f \in \mathscr{F}} \mathbb{E}\left[d\left(\widehat{f}_n, f\right)\right] \geq c s_n$$

where $c > 0$ and $s_n \to 0$ as $n \to \infty$. The inf is taken over all estimators, i.e. all measurable functions $\widehat{f}_n : \mathscr{Z} \to \mathscr{S}$.

Suppose we have shown that
Equation:

$$\liminf_{n \to \infty} s_n^{-1} \mathscr{R}_n^* \geq c > 0 \qquad \text{(A lower bound)}$$

and also that for a particular estimator $\overline{f}_n$
Equation:

$$\limsup_{n \to \infty} s_n^{-1} \sup_{f \in \mathscr{F}} \mathbb{E}_f\left[d\left(\overline{f}_n, f\right)\right] \leq C$$

Equation:

$$\Rightarrow \limsup_{n \to \infty} s_n^{-1} \mathscr{R}_n^* \leq C,$$

We say that s_n is the optimal rate of convergence for this problem and that $\overline{f}_n$ attains that rate.

Note: Two rates of convergence Ψ_n and Ψ_n' are equivalent, i.e. $\Psi_n \equiv \Psi_n'$ iff

Equation:

$$0 < \liminf_{n \to \infty} \frac{\Psi_n}{\Psi_n'} \leq \limsup_{n \to \infty} \frac{\Psi_n}{\Psi_n'} < \infty$$

General Reduction Scheme

Instead of directly bounding the expected performance, we are going to prove stronger probability bounds of the form
Equation:

$$\inf_{\widehat{f}_n} \sup_{f \in \mathscr{F}} \mathscr{P}_f \left(d\left(\widehat{f}_n, f\right) \geq s_n \right) \geq c > 0$$

These bounds can be readily converted to expected performance bounds using Markov's inequality:
Equation:

$$\mathscr{P}_f \left(d\left(\widehat{f}_n, f\right) \geq s_n \right) \leq \frac{\mathbb{E}_f \left[d\left(\widehat{f}_n, f\right) \right]}{s_n}$$

Therefore it follows:
Equation:

$$\inf_{\widehat{f}_n} \sup_{f \in \mathscr{F}} \mathbb{E}_f \left[d\left(\widehat{f}_n, f\right) \right] \geq \inf_{\widehat{f}_n} \sup_{f \in \mathscr{F}} s_n \mathscr{P}_f \left(d\left(\widehat{f}_n, f\right) \geq s_n \right) \geq c s_n$$

First Reduction Step

Reduce the original problem to an easier one by replacing the larger class $\mathscr{F}$ with a smaller finite class $\{f_0, \cdots, f_M\} \subseteq \mathscr{F}$. Observe that
Equation:

$$\inf_{\widehat{f}_n} \sup_{f \in \mathscr{F}} \mathscr{P}_f \left(d\left(\widehat{f}_n, f\right) \geq s_n \right) \geq \inf_{\widehat{f}_n} \sup_{f \in \{f_0, \cdots, f_M\}} \mathscr{P}_f \left(d\left(\widehat{f}_n, f\right) \geq s_n \right)$$

The key idea is to choose a finite collection of models such that the resulting problem is as hard as the original, otherwise the lower bound will not be tight.

Second Reduction Step

Next, we reduce the problem to a hypotheses test. Ideally, we would like to have something like
Equation:

$$\inf_{\widehat{f}_n} \sup_{f \in \mathscr{F}} \mathscr{P}_f \left(d\left(\widehat{f}_n, f\right) \geq s_n \right) \geq \inf_{\widehat{f}_n} \sup_{j \in \{0, \cdots, M\}} \mathscr{P}_{f_j} \left(\widehat{h}_n\left(Z\right) \neq j \right)$$

The inf is over all measurable test functions
Equation:

$$\widehat{h}_n : \mathscr{Z} \to \{0, \cdots, M\}$$

and $\mathscr{P}_{f_j}\left(\widehat{h}_n\left(Z\right) \neq j\right)$ denotes the probability that after observing the data, the test infers the wrong hypothesis.

This might not always be true or easy to show, but in certain scenarios it can be done. Suppose $d(.,.)$ is a semi-distance, i.e. it satisfies

- **(i)**$d(f,g) = d(g,f) \geq 0$ (Symmetric)
- **(ii)**
  Equation:

$$d(f,f) = 0$$

- **(iii)**$d(f,g) \leq d(h,f) + d(h,g)$ (Triangle inequality)

E.g. with $f, g : \mathbb{R}^d \to \mathbb{R}, d\left(f,g\right) \overset{\Delta}{=} ||f-g||_2$.
Lemma

Suppose $d(.,.)$ is a semi-distance. Also suppose that we have constructed $f_0, \cdots, f_M$ s.t.
$d\left(f_j, f_k\right) \geq 2s_n, \forall j \neq k$. Take any estimator $\widehat{f}_n$ and define the test: $\Psi^* \circ \widehat{f}_n : \mathscr{Z} \to \{0, \cdots, M\}$ as
Equation:

$$\Psi^*\left(\widehat{f}_n\right) = \underset{j}{\operatorname{argmin}}\, d\left(\widehat{f}_n, f_j\right)$$

Then $\Psi^*\left(\widehat{f}_n\right) \neq j$, implies $d\left(\widehat{f}_n, f_j\right) \geq s_n$.

Suppose $\Psi^*\left(\widehat{f}_n\right) \neq j \iff \exists k \neq j : d\left(\widehat{f}_n, f_k\right) \leq d\left(\widehat{f}_n, f_j\right)$. Now
Equation:

$$2s_n \leq d\left(f_j, f_k\right) \leq d\left(\widehat{f}_n, f_j\right) + d\left(\widehat{f}_n, f_k\right) \leq 2d\left(\widehat{f}_n, f_j\right)$$

Equation:

$$\Rightarrow d\left(\widehat{f}_n, f_j\right) \geq s_n$$

The previous lemma implies that
Equation:

$$\mathscr{P}_{f_j}\left(d\left(\widehat{f}_n, f_j\right) \geq s_n\right) \geq \mathscr{P}_{f_j}\left(\Psi^*\left(\widehat{f}_n\right) \neq j\right)$$

Therefore,
Equation:

$$\begin{aligned}\inf_{\widehat{f}_n}\sup_{f\in\mathscr{F}}\mathscr{P}_{f_j}\left(d\left(\widehat{f}_n,f_j\right)\geq s_n\right) &\geq \inf_{\widehat{f}_n}\max_{f\in\{f_0,\cdots,f_M\}}\mathscr{P}_{f_j}\left(d\left(\widehat{f}_n,f_j\right)\geq s_n\right)\\ &\geq \inf_{\widehat{f}_n}\max_{j\in\{0,\cdots,M\}}\mathscr{P}_{f_j}\left(\Psi^*\left(\widehat{f}_n\right)\neq j\right)\\ &\geq \inf_{\widehat{h}_n}\max_{j\in\{0,\cdots,M\}}\mathscr{P}_{j}\left(\widehat{h}_n\neq j\right)\\ &\stackrel{\Delta}{=} P_{e,M}\end{aligned}$$

The third step follows since we are replacing the class of tests defined by $\Psi^*\left(\widehat{f}_n\right)$ by a larger class of ALL possible tests $\widehat{h}_n$, and hence the $\inf$ taken over the larger class is smaller.

Now our goal throughout is going to be to find lower bounds for $P_{e,M}$.

So we need to construct $f_0,\cdots,f_M$ s.t. $d\left(f_j,f_k\right)\geq 2s_n$, $j\neq k$ and $P_{e,M}\geq c>0$. Observe that this requires careful construction since the first condition necessitates that f_j and f_k are far from each other, while the second condition requires that f_j and f_k are close enough so that it is harder to distinguish them based on a given sample of data, and hence the probability of error $P_{e,M}$ is bounded away from 0.

We now try to lower bound the probability of error $P_{e,M}$. We first consider the case $M=1$, corresponding to binary hypothesis testing.

M = 1: Let P_0 and P_1 denote the two probability measures, i.e. distributions of the data under models 0 and 1. Clearly if P_0 and P_1 are very “close", then it is hard to distinguish the two hypotheses, and so $P_{e,1}$ is large.

A natural measure between probability measures is the total variation , defined as:
Equation:

$$V\left(P_0,P_1\right)=\sup_A\left|P_0\left(A\right)-P_1\left(A\right)\right|=\sup_A\left|\int_A p_0\left(Z\right)-p_1\left(Z\right)d\nu\left(Z\right)\right|$$

where p_0 and p_1 are the densities of P_0 and P_1 with respect to a common dominating measure ν and A is any subset of the domain. We will lower bound the probability of error $P_{e,1}$ using the total variation distance. But first, we establish the following lemma.
Lemma
Scheffe's lemma
Equation:

$$\begin{aligned}V(P_0,P_1) &= \frac{1}{2}\int\left|p_0\left(Z\right)-p_1\left(Z\right)\right|d\nu\left(Z\right)=\frac{1}{2}\int\left|p_0-p_1\right|\\ &= 1-\int\min\left(p_0,p_1\right)\end{aligned}$$

Recall the definition of the total variation distance:
Equation:

$$V\left(P_0,P_1\right)=\sup_A\left|\int_A p_0-p_1\right|$$

Observe that the set A maximizing the right hand side is given by either $\{Z\in\mathscr{Z}:p_0\left(Z\right)\geq p_1\left(Z\right)\}$ or $\{Z\in\mathscr{Z}:p_1\left(Z\right)\geq p_0\left(Z\right)\}$.

Let us pick $A_0=\{Z\in\mathscr{Z}:p_0\left(Z\right)\geq p_1\left(Z\right)\}$. Then
Equation:

$$V\left(P_0,P_1\right)=\int_{A_0}p_0-p_1=-\int_{A_0^c}p_0-p_1=\frac{1}{2}\int\left|p_0-p_1\right|$$

For the second part, notice that
Equation:

$$p_0\left(Z\right)-\min\left(p_0\left(Z\right),p_1\left(Z\right)\right)=\begin{cases}0 & \text{if } p_0\left(Z\right)\leq p_1\left(Z\right)\\ p_0\left(Z\right)-p_1\left(Z\right) & \text{if } p_0\left(Z\right)\geq p_1\left(Z\right)\end{cases}$$

Now consider
Equation:

$$1-\int\min\left(p_0,p_1\right)=\int p_0\left(Z\right)-\min\left(p_0\left(Z\right),p_1\left(Z\right)\right)=\int_{A_0}p_0\left(Z\right)-p_1\left(Z\right)d\nu\left(Z\right)=V\left(P_0,P_1\right)$$

We are now ready to tackle the lower bound on $P_{e,1}$. In this case, we consider all tests $\widehat{h}_n\left(Z\right):\mathscr{Z}\to\{0,1\}$. Equivalently, we can define $\widehat{h}_n\left(Z\right)=1_A\left(Z\right)$, where A is any subset of the domain.
Equation:

$$\begin{aligned}P_{e,1}=\inf_{\widehat{h}_n}\max_{j\in\{0,\cdots,M\}}\mathscr{P}_j\left(\widehat{h}_n\neq j\right) &\geq \inf_{\widehat{h}_n}\left(\frac{1}{2}P_0\left(\widehat{h}_n\neq 0\right)+P_1\left(\widehat{h}_n\neq 1\right)\right)\\ &= \frac{1}{2}\inf_A P_0\left(1_A\left(Z\right)\neq 0\right)+P_1\left(1_A\left(Z\right)\neq 1\right)\\ &= \frac{1}{2}\inf_A P_0\left(A\right)+P_1\left(A^c\right)\\ &= \frac{1}{2}\inf_A 1-\left(P_1\left(A\right)-P_0\left(A\right)\right)\\ &= \frac{1}{2}(1-V\left(P_0,P_1\right))\end{aligned}$$

So if P_0 is close to P_1, then $V(P_0,P_1)$ is small and the probability of error $P_{e,1}$ is large.

This is interesting, but unfortunately, it is hard to work with total variation, especially for multivariate distributions. Bounds involving the Kullback-Leibler divergence are much more convenient.

Equation:

$$K(P_1 \,||P_0\Big) = \int \log \frac{p_1\left(Z\right)}{p_0\left(Z\right)} p_1\left(Z\right) d\nu\left(Z\right) = \int \log \frac{p_1}{p_0} p_1$$

The following Lemma relates total variation, affinity and KL divergence.
Lemma

$1 - V\left(P_0, P_1\right) \geq \frac{1}{2} A^2\left(P_0, P_1\right) \geq \frac{1}{2} \exp\left(-K(P_1 \,||P_0\,)\right)$

For the first inequality,
Equation:

$$\begin{aligned}
A^2\left(P_0, P_1\right) &= \left(\int \sqrt{p_0 p_1}\right)^2 \\
&= \left(\int \sqrt{\min\left(p_0, p_1\right) \max\left(p_0, p_1\right)}\right)^2 \\
&= \left(\int \sqrt{\min\left(p_0, p_1\right)} \sqrt{\max\left(p_0, p_1\right)}\right)^2 \\
&\leq \int \min\left(p_0, p_1\right) \int \max\left(p_0, p_1\right) && \text{by Cauchy-Schwarz inequality} \\
&= \int \min\left(p_0, p_1\right) \left(2 - \int \min\left(p_0, p_1\right)\right) && \because \int \min(p_0,p_1) + \int \max(p_0,p_1) = \int p_0 + \int p_1 = 2 \\
&\leq 2 \int \min\left(p_0, p_1\right) \\
&= 2(1 - V\left(P_0, P_1\right))
\end{aligned}$$

For the second inequality,
Equation:

$$
\begin{aligned}
A^2\left(P_0, P_1\right) &= \left(\int \sqrt{p_0 p_1}\right)^2 \\
&= \exp\left(\log\left(\int \sqrt{p_0 p_1}\right)^2\right) \\
&= \exp\left(2\log\left(\int \sqrt{p_0 p_1}\right)\right) \\
&= \exp\left(2\log\left(\int \sqrt{\frac{p_0}{p_1}} p_1\right)\right) \\
&\geq \exp\left(2\int \log\left(\sqrt{\frac{p_0}{p_1}}\right) p_1\right) \qquad \text{by Jensen's inequality} \\
&= \exp\left(-\int \log\left(\sqrt{\frac{p_1}{p_0}}\right) p_1\right) \\
&= \exp\left(-K(P_1 \,||P_0\,)\right)
\end{aligned}
$$

Putting everything together, we now have the following Theorem:
Theorem

Let $\mathscr{F}$ be a class of models, and suppose we have observations Z distributed according to $\mathscr{P}_f$, $f \in \mathscr{F}$. Let $d\left(\widehat{f}_n, f\right)$ be the performance measure of the estimator $\widehat{f}_n\left(Z\right)$ relative to the true model f. Assume also $d(.\,,.\,)$ is a semi-distance. Let $f_0, f_1 \in \mathscr{F}$ be s.t. $d\left(f_0, f_1\right) \geq 2s_n$. Then
Equation:

$$
\begin{aligned}
\inf_{\widehat{f}_n} \sup_{f \in \mathscr{F}} \mathscr{P}_f\left(d\left(\widehat{f}_n, f\right) \geq s_n\right) &\geq \inf_{\widehat{f}_n} \max_{j \in \{0,1\}} \mathscr{P}_{f_j}\left(d\left(\widehat{f}_n, f_j\right) \geq s_n\right) \\
&\geq \frac{1}{4}\exp\left(-K(P_{f_1}\,||P_{f_0}\,)\right)
\end{aligned}
$$

How do we use this theorem?

Choose f_0, f_1 such that $K(P_1||P_0) \leq \alpha$, then $P_{e,1}$ is bounded away from 0 and we get a bound
Equation:

$$
\inf_{\widehat{f}_n} \sup_{f \in \mathscr{F}} \mathscr{P}_f\left(d\left(\widehat{f}_n, f\right) \geq s_n\right) \geq c > 0
$$

or, after Markov's
Equation:

$$
\inf_{\widehat{f}_n} \sup_{f \in \mathscr{F}} \mathbb{E}_f\left[d\left(\widehat{f}_n, f\right)\right] \geq c s_n
$$

To apply the theorem, we need to design f_0, f_1 s.t. $d\left(f_0, f_1\right) \geq 2 s_n$ and $\exp\left(-K(P_{f_1}||P_{f_0})\right) > 0$. To reiterate, the design of f_0, f_1 requires careful construction so as to balance the tradeoff between the first condition which requires f_0, f_1 to be far apart, and the second condition which requires f_0, f_1 to be close to each other.

Example:
Lets use this theorem in a problem we are familiar with. Let $X \in [0,1]$ and $Y|X = x \sim \text{Bernoulli}(\eta(x))$, where $\eta(x) = P(Y = 1|X = x)$.
Suppose $G^* = \left[t^*, 1\right]$. We proved that under these assumptions and an upper bound on the density of X, the Chernoff bounding technique yielded an expected error rate for ERM
Equation:

$$\mathbb{E}\left[R\left(\widehat{G}_n\right) - R^*\right] = O\left(\sqrt{\frac{\log n}{n}}\right)$$

Is this the best possible rate?
Construct two models in the above class (denote it by $\mathscr{P}$), $P_{XY}^{(0)}$ and $P_{XY}^{(1)}$. For both take $P_X \sim \text{Uniform}\left([0,1]\right)$ and $\eta_{(0)} = 1/2 - a$, $\eta_{(1)} = 1/2 + a (a > 0)$, so $G_0^* = \emptyset$, $G_1^* = [0,1]$.
We are interested in controlling the excess risk
Equation:

$$R\left(\widehat{G}_n\right) - R\left(G^*\right) = \int_{\widehat{G}_n \Delta G^*} |2\eta\left(x\right) - 1| dP_X\left(x\right)$$

Note that if the true underlying model is either $P_{XY}^{(0)}$ or $P_{XY}^{(1)}$, we have:
Equation:

$$R_j\left(\widehat{G}_n\right) - R_j\left(G_j^*\right) = \int_{\widehat{G}_n \Delta G_j^*} |2\eta_j\left(x\right) - 1| dx = 2a \int_{\widehat{G}_n \Delta G_j^*} dx = 2a d_\Delta\left(\widehat{G}_n, G_j^*\right)$$

Proposition 1
$d_\Delta\left(.,.\right)$ is a semi-distance.

It suffices to show that $d\left(G_1, G_2\right) = d\left(G_2, G_1\right) \geq 0$, $d(G,G) = 0 \forall G$ and $d\left(G_1, G_2\right) \leq d\left(G_1, G_3\right) + d\left(G_3, G_2\right)$. The first two statements are obvious. The last one (triangle inequality) follows from the fact that $G_1 \Delta G_2 \subseteq \left(G_1 \Delta G_3\right) \cup \left(G_3 \Delta G_2\right)$.

Suppose this was not the case, then $\exists x : x \in G_1 \Delta G_2$ s.t. $x \notin G_1 \Delta G_3$ and $x \notin G_2 \Delta G_3$. In other words,
Equation:

$$x \in \left(G_1 \Delta G_2\right) \cap \left(G_1 \Delta G_3\right)^c \cap \left(G_2 \Delta G_3\right)^c$$

Since $S \Delta T = (S \cap T^c) \cup (S^c \cap T)$, we have:
Equation:

$$\begin{aligned} x &\in [(G_1 \cap G_2^c) \cup (G_1^c \cap G_2)] \cap [(G_1^c \cup G_3) \cap (G_1 \cup G_3^c)] \cap [(G_2^c \cup G_3) \cap (G_2 \cup G_3^c)] \\ &\in [G_1 \cap (G_1^c \cup G_3) \cap G_2^c \cap (G_2 \cup G_3^c)] \cup [G_1^c \cap (G_1 \cup G_3^c) \cap G_2 \cap (G_2^c \cup G_3)] \\ &\in [G_1 \cap G_3 \cap G_2 \cap G_3^c] \cup [G_1^c \cap G_3^c \cap G_2 \cap G_3] \\ &\in \emptyset, \text{ a contradiction} \end{aligned}$$

Lets look at the first reduction step:
Equation:

$$\begin{aligned} \inf_{\widehat{G}_n} \sup_{p \in \mathscr{P}} P\left(R\left(\widehat{G}_n\right) - R\left(G^*\right) \geq s_n\right) &\geq \inf_{\widehat{G}_n} \max_{j \in \{0,1\}} P_j\left(R_j\left(\widehat{G}_n\right) - R_j\left(G_j^*\right) \geq s_n\right) \\ &= \inf_{\widehat{G}_n} \max_{j \in \{0,1\}} P_j\left(d_\Delta\left(\widehat{G}_n, G_j^*\right) \geq s_n/2a\right) \end{aligned}$$

So we can work out a bound on d_Δ and then translate it to excess risk.

Lets apply Theorem 1. Note that $d_\Delta\left(G_0^*, G_1^*\right) = 1$ and let $P_0 \overset{\Delta}{=} P^{(0)}_{X_1,Y_1,\cdots,X_n,Y_n}$ and $P_1 \overset{\Delta}{=} P^{(1)}_{X_1,Y_1,\cdots,X_n,Y_n}$.
Equation:

$$\begin{aligned} K(P_1||P_0) &= \mathbb{E}_1\left[\log \frac{p^{(1)}_{X_1,Y_1,\cdots,X_n,Y_n}(X_1,Y_1,\cdots,X_n,Y_n)}{p^{(0)}_{X_1,Y_1,\cdots,X_n,Y_n}(X_1,Y_1,\cdots,X_n,Y_n)}\right] \\ &= \mathbb{E}_1\left[\log \frac{p^{(1)}_{X_1,Y_1}(X_1,Y_1)\cdots p^{(1)}_{X_n,Y_n}(X_n,Y_n)}{P^{(0)}_{X_1,Y_1}(X_1,Y_1)\cdots p^{(0)}_{X_n,Y_n}(X_n,Y_n)}\right] \\ &= \sum_{i=1}^n \mathbb{E}_1\left[\log \frac{p^{(1)}_{X_i,Y_i}(X_i,Y_i)}{p^{(0)}_{X_i,Y_i}(X_i,Y_i)}\right] \\ &= n\mathbb{E}_1\left[\log \frac{p^{(1)}_{Y|X}(Y_1|X_1)}{p^{(0)}_{Y|X}(Y_1|X_1)}\right] \end{aligned}$$

Now $p^{(1)}_{Y|X}(Y_1 = 1|X_1) = 1/2 + a$ and $p^{(0)}_{Y|X}(Y_1 = 1|X_1) = 1/2 - a$. Also under model 1, $Y_1 \sim \text{Bernoulli}\,(1/2 + a)$. So we get:
Equation:

$$
\begin{aligned}
K(P_1||P_0) &= n\left[(1/2+a)\log\frac{1/2+a}{1/2-a}+(1/2-a)\log\frac{1/2-a}{1/2+a}\right] \\
&= n[2a\log(1/2+a)-2a\log(1/2-a)] \\
&= 2na\log\frac{1/2+a}{1/2-a} \\
&\leq 2na\left(\frac{1/2+a}{1/2-a}-1\right) \\
&= 4na^2\frac{1}{1/2-a}
\end{aligned}
$$

Let $a=1/\sqrt{n}$ and $n\geq 16$, then $K(P_1\,||P_0)\leq 4n\frac{1}{n}\frac{1}{1/2-1/\sqrt{n}}\leq 16$.

Using Theorem 1, since $d_{\Delta}\left(G_0^*,G_1^*\right)=1$, we get:
Equation:

$$
\inf_{\widehat{G}_n}\max_j P_j\left(d_{\Delta}\left(\widehat{G}_n,G_j^*\right)\geq 1/2\right)\geq\frac{1}{4}e^{-16}
$$

Taking $s_n=1/\sqrt{n}$, this implies
Equation:

$$
\inf_{\widehat{G}_n}\sup_{p\in\mathscr{P}} P\left(R\left(\widehat{G}_n\right)-R\left(G^*\right)\geq 1/\sqrt{n}\right)\geq\frac{1}{4}e^{-16}
$$

or, after Markov's inequality
Equation:

$$
\inf_{\widehat{G}_n}\sup_{p\in\mathscr{P}}\mathbb{E}\left[R\left(\widehat{G}_n\right)-R\left(G^*\right)\right]\geq\frac{1}{4}e^{-16}\frac{1}{\sqrt{n}}
$$

Therefore, apart from the log n factor, ERM is getting the best possible performance.

Reducing the initial problem to a binary hypothesis testing does not always work. Sometimes we need M hypotheses, with $M\to\infty$ as $n\to\infty$. If this is the case, we have the following theorem:

Theorem 2 Let $M\geq 2$. $\{f_0,\cdots,f_M\}\in\mathscr{F}$ be such that

- .$d\left(f_j,f_k\right)\geq 2s_n$, where d is a semi-distance.
- .$\frac{1}{M}\sum_{j=1}^{M}K(P_j\,||P_0)\leq\alpha\log M$, with $0<\alpha<1/8$.

Then
Equation:

$$\begin{aligned}\inf_{\widehat{f}_n}\sup_{f\in\mathscr{F}} P_f\left(d\left(\widehat{f}_n,f\right)\geq s_n\right) &\geq \inf_{\widehat{f}_n}\max_j P_j\left(d\left(\widehat{f}_n,f_j\right)\geq s_n\right)\\ &\geq \frac{\sqrt{M}}{1+\sqrt{M}}\left(1-2\alpha-2\sqrt{\frac{\alpha}{\log M}}\right)>0\end{aligned}$$

We will use this theorem to show that the estimator of Lecture 4 is optimal. Recall the setup of Lecture 4. Let
Equation:

$$\mathscr{F}=\{f:|f(t)-f(s)|\leq L|t-s|\forall t,s\}$$

i.e. the class of Lipschitz functions with constant L. Let
Equation:

$$x_i=i/n,\qquad i=1,\cdots,n$$

Equation:

$$Y_i=f\left(x_i\right)+W_i$$

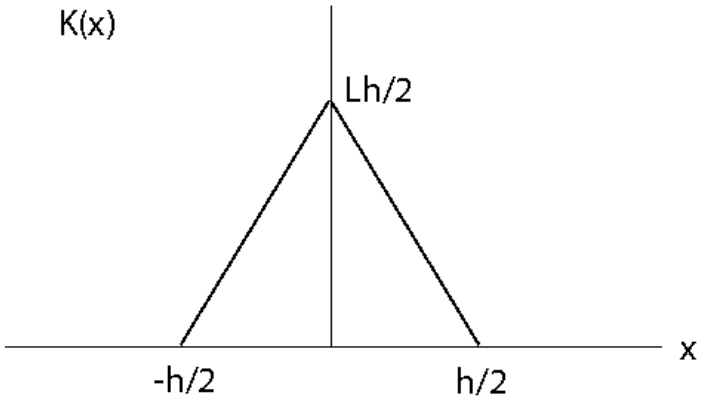
$\mathbb{E}\left[W_i\right]=0,\mathbb{E}\left[W_i^2\right]=\sigma^2<\infty,W_i,W_j\ \text{are indepedent if}\ i\neq j$. In that lecture, we constructed an estimator $\widehat{f}_n$ such that
Equation:

$$\sup_{f\in\mathscr{F}}\mathbb{E}[||\widehat{f}_n-f||^2]=O\left(n^{-2/3}\right)$$

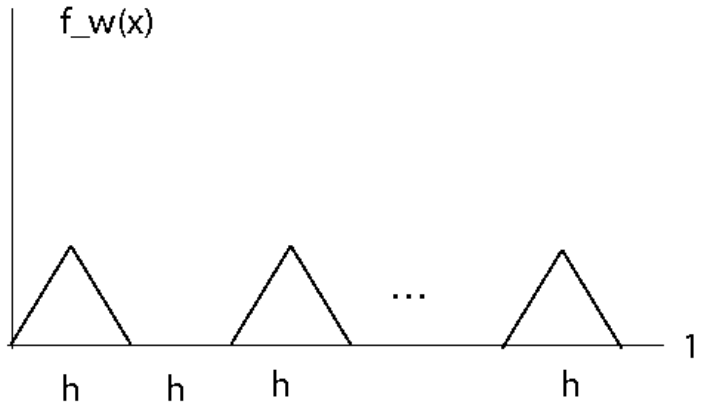
Is this the best we can do?

We are going to construct a collection $f_0,\cdots,f_M\in\mathscr{F}$ and apply Theorem 2. Notice that the metric of interest is $d\left(\widehat{f}_n,f\right)=||\widehat{f}_n-f\,||$, a semi-distance. Let $W_i\overset{iid}{\sim}\mathscr{N}\left(0,\sigma^2\right)$. Let $m\in\mathbb{N}$, $h=1/m$ and define
Equation:

$$K\left(x\right)=\left(\frac{Lh}{2}-L\left|x\right|\right)\mathbb{I}_{|x|\leq h/2}=\frac{L}{2}|h-2x|\mathbb{I}_{|x|\leq h/2}$$



Note that $|K(a) - K(b)| \leq L|a - b|, \forall a, b$. The subclass we are going to consider are functions of the form



i.e. “bump" functions. Let $\Omega = \{0, 1\}^m$ be the collection of binary vectors of length m, e.g. $w = (1, 0, 1, \cdots, 0) \in \Omega$. Define

Equation:

$$f_w(x) = \sum_{i=1}^{m} w_i K\left(x - \frac{h}{2}(2i - 1)\right)$$

Note that for $w, w' \in \Omega$,

Equation:

$$d\left(f_w, f_{w'}\right) = ||f_w - f_{w'}|| = \left(\int_0^1 \sum_{i=1}^m \left(w_i - w_i'\right)^2 K^2\left(x - \frac{h}{2}\left(2i-1\right)\right)\right)^{1/2}$$
$$= \sqrt{\rho(w,w')}\sqrt{\int K^2\left(x\right)dx}$$

where $\rho(w,w')$ is the Hamming distance, $\rho\left(w,w'\right) = \sum_{i=1}^m \left|w_i - w_i'\right|^2 = \sum_{i=1}^m \left|w_i - w_i'\right|$. Now
Equation:

$$\int K^2\left(x\right) = 2\int_0^{h/2} L^2x^2dx = 2L^2\frac{h^3}{3\cdot 8} = \frac{L^2}{12}h^3$$

so
Equation:

$$d\left(f_w, f_{w'}\right) = \sqrt{\rho(w,w')}\frac{L}{\sqrt{12}}h^{3/2}$$

Since $|\Omega| = 2^n$, the number of functions in our class is 2^n. Turns out, we do not need to consider all functions $f_w, w \in \Omega$, but only a select few. Using all the functions leads to a looser lower bound of the form n^{-1}, which corresponds to the parametric rate. The problem under consideration is non-parametric, and hence we expect a slower rate of convergence. To get a tighter lower bound, the following result is of use:
Lemma
Varshamov-Gilbert '62

Let $m \geq 8$. There exists a subset $\left\{w^{(0)}, \cdots, w^{(M)}\right\}$ of Ω such that $w^{(0)} = (0, 0, \cdots, 0)$,
Equation:

$$\rho\left(w^{(j)}, w^{(k)}\right) \geq \frac{m}{8}, \quad \forall 0 \leq j < k \leq M \text{ and } M \geq 2^{m/8}.$$

What this lemma says is that there are many $(\sim 2^m)$ sequences in Ω that are very different (i.e. $\rho\left(w^{(j)}, w^{(k)}\right) \sim m$). We are going to use the lemma to construct a useful set of hypotheses. Let $\left\{w^{(0)}, \cdots, w^{(M)}\right\}$ be the class of sequences in the lemma and define
Equation:

$$f_j \overset{\Delta}{=} f_{w^{(j)}}, \quad j \in \{0, \cdots, M\}$$

We now need to look at the conditions of Theorem 2 and choose m appropriately.

First note that for $j \neq k$,
Equation:

$$d\left(f_j, f_k\right) = \sqrt{\rho\left(w^{(j)}, w^{(k)}\right)}\frac{L}{\sqrt{12}}h^{3/2} \geq \sqrt{\frac{m}{8}}\frac{L}{\sqrt{12}}m^{-3/2} = \frac{L}{4\sqrt{6}}m^{-1}$$

Now let $P_j \overset{\Delta}{=} P^{(j)}_{Y_1,\cdots,Y_m}, j \in \{0,\cdots,M\}$. Then
Equation:

$$\begin{aligned} K(P_j||P_0) &= \mathbb{E}_j\left[\log\frac{p^{(j)}_{Y_1,\cdots,Y_m}}{p^{(0)}_{Y_1,\cdots,Y_m}}\right] \\ &= \sum_{i=1}^{n}\mathbb{E}_j\left[\log\frac{p^{(j)_{Y_i}}}{p^{(0)}_{Y_i}}\right] = \frac{1}{2\sigma^2}\sum_{i=1}^{n}f_j^2\left(x_i\right) \\ &\leq \frac{1}{2\sigma^2}\sum_{i=1}^{n}\left(\frac{Lh}{2}\right)^2 = \frac{L^2}{8\sigma^2}nh^2 = \frac{L^2}{8\sigma^2}nm^{-2} \end{aligned}$$

Now notice that $\log M \geq \frac{m}{8}\ \log 2$ (from Lemma [link]). We want to choose m such that
Equation:

$$\frac{1}{M}\sum_{j=1}^{M}K(P_j\,||P_0) \leq \frac{L^2}{8\sigma^2}nm^{-2} < \alpha\frac{m}{8}\ \log 2 \leq \alpha\log M$$

This gives
Equation:

$$m > \left(\frac{L^2}{\alpha\sigma^2\ \log 2}\right)^{1/3}n^{1/3} := C_0n^{1/3}$$

so take $m = \left\lfloor C_0n^{1/3} + 1\right\rfloor$. Now
Equation:

$$d\left(f_j, f_k\right) \geq \frac{L}{4\sqrt{6}}m^{-1} \geq 2\text{const}\ \ n^{-1/3} \qquad \text{for}\ \ n \geq n_0\left(\text{const}\right)$$

Therefore,
Equation:

$$\inf_{\widehat{f}_n}\sup_{f\in\mathscr{F}}P_f\left(||\widehat{f}_n - f|| \geq \text{const}\ \ n^{-1/3}\right) \geq c > 0$$

or,
Equation:

$$\inf_{\widehat{f}_n} \sup_{f \in \mathscr{F}} P_f \left(||\widehat{f}_n - f||^2 \geq \text{const } n^{-2/3} \right) \geq c > 0$$

or after Markov's inequality,
Equation:

$$\inf_{\widehat{f}_n} \sup_{f \in \mathscr{F}} \mathbb{E}_f \left[||\widehat{f}_n - f||^2 \right] \geq c \cdot \text{const } n^{-2/3}$$

Therefore, the estimator constructed in class attains the optimal rate of convergence.